n°34 Octobre 2022
#34 October 2022

Lexing Insights

Le réseau Lexing® vous informe – The Lexing® network informs you

RETOUR SUR LA CONFERENCE MONDIALE DU RESEAU LEXING
LEXING NETWORK WORLD CONFERENCE HIGHLIGHTS

INTELLIGENCE ARTIFICIELLE ET METAVERS : ASPECTS JURIDIQUES

- La 1ère Conférence mondiale 2022 du réseau Lexing s'est tenue, en mode virtuel, le 8 juin 2022. Au cours de cette conférence, les membres du réseau y ont discuté tout d'abord du cadre européen et mondial pour encadrer l'IA et particulièrement du projet de règlement de l'UE qui vise à garantir une IA digne de confiance. Ils ont décrypté le métavers, ce nouvel univers parallèle dont les contours restent encore flous, mais qui pose d'ores et déjà de multiples enjeux juridiques et éthiques, et se sont interrogés sur la pertinence de la création d'un droit des métavers.
- En marge de cette conférence mondiale, ont également été organisées, en présentiel et/ou en distanciel, par les membres du réseau, des conférences régionales dédiées à l'état du droit de l'IA, des métavers, des robots ou encore des données personnelles des Etats-Unis au Japon en passant par l'Europe et l'Afrique.
- Le présent numéro de Lexing Insights présente une sélection des interventions réalisées à l'occasion de ces différents évènements et en dégage les points saillants en vue de vous offrir un panorama des thématiques abordées. Bonne lecture !

Les pays suivants ont contribué à ce numéro : Afrique du Sud, Australie, Belgique, Chine, Espagne, Etats-Unis, France, Grèce, Japon.

ARTIFICIAL INTELLIGENCE AND METAVERSE : LEGAL ASPECTS

- The first Lexing World Conference was held online on 8 June 2022 on the theme "Artificial Intelligence and Metaverse: Legal aspects". *During the conference, the network members first analyzed the European and global framework for Artificial Intelligence, with focus on the draft European Regulation that aims to ensure trustworthy AI. Then they reviewed the metaverse, this new parallel universe whose nature and content are still unclear, but which already raises multiple legal and ethical issues, and discussed the relevance of a metaverse law.*
- *In conjunction with this world conference, in person and/or online regional conferences dedicated to the state of the law on AI, metaverse, robots, or personal data at regional or local level from the United States to Japan via Europe and Africa were also organized by the network members.*
- *This issue of the Lexing Insights contains key insights and highlights from these events. Happy reading!*

The following countries have contributed to this issue: Australia, Belgium, China, France, Greece, Japan, South Africa, Spain, United States.

Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leurs pays respectifs.

Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

https://lexing.network

FREDERIC FORSTER
Vice-président du réseau Lexing® et Directeur du pôle Industries et services informatiques, télécoms et bancaires du cabinet Lexing Alain Bensoussan-Avocats

VP of Lexing® network and Head of the Industries & IT, Telecoms and Banking Services division of Lexing Alain Bensoussan-Avocats

AFRIQUE DU SUD

MICHALSONS

La Conférence sud-africaine « Lexverse »

▪ Le 8 juin 2022, le cabinet Michalsons a organisé, en Afrique du Sud, sa première conférence « Lexverse » **(1)**, dédiée à l'univers juridique du numérique, de la data et des technologies émergentes. Ce fut l'occasion de rencontres, de réflexions et d'échanges autour de thèmes d'actualité **(2)**. Il s'agissait d'un événement hybride, auquel des participants du monde entier ont pu assister à la fois en présentiel et en distanciel.

▪ Cette conférence a réuni des experts juridiques de premier plan, mondialement reconnus **(3)**, pour discuter des technologies émergentes (de l'IA au métavers, en passant par la blockchain et la réalité virtuelle) et de leurs réglementations possibles ou existantes.

▪ Sont notamment intervenus lors de la conférence John Giles (cabinet Michalsons), Mike Abel (fondateur et directeur de l'agence M&C Saatchi Abel), Alain Bensoussan et Frédéric Forster (Lexing Alain Bensoussan).

Droit et réglementation de la réalité virtuelle

▪ Le droit de la réalité virtuelle est en plein développement.

▪ **Le cabinet Michalsons présent dans le métavers.** Le cabinet Michalsons a désormais des bureaux virtuels dans le métavers, diversifiant ainsi ses méthodes de contact et de rencontre afin d'accompagner ses clients selon leur mode de communication préféré, qu'il soit physique, en ligne ou virtuel.

▪ **Le futur monde de la réalité mixte.** Notre futur sera fait d'un monde de réalité mixte, où la réalité augmentée (AR) et la réalité mixte (RM) vont s'insérer entre le virtuel d'un côté et le réel de l'autre. Les acteurs économiques l'ont d'ailleurs bien compris : Facebook s'est rebaptisée Meta **(4)**. Microsoft a acquis l'éditeur de jeux vidéo Activision **(5)** et Apple va bientôt lancer son casque de réalité virtuelle **(6)**.

▪ **Cadre juridique de la réalité virtuelle.** Existe-t-il des lois virtuelles ? Quelles lois s'appliquent dans le monde virtuel ? Comment allons-nous encadrer juridiquement la réalité numérique ? Autant de questions essentielles auxquelles il sera bientôt urgent de répondre.

▪ Il n'existe actuellement pas de législation sur la réalité virtuelle (alors qu'il existe une législation sur l'intelligence artificielle par exemple **(7)**), et il est peu probable qu'il y en ait un jour, car les lois existantes applicables au monde réel étant souvent rédigées de manière à être technologiquement neutres et formulées selon des grands principes, elles sont de ce fait transposables au monde virtuel. A ces textes de loi s'ajouteront les conditions d'utilisation et diverses politiques établies par les propriétaires de mondes virtuels. Prenons quelques exemples concrets pour observer la manière dont les lois existantes pourraient s'appliquer à la réalité virtuelle :

- un avatar serait probablement qualifié de personne physique en vertu des lois existantes, et non de personne morale. Il ne s'agirait pas non plus d'une personne robot, un nouveau type de personne juridique qui devrait,

REFERENCES

(1) https://thelexverse.com/

(2) Infographie Conférence Lexverse

(3) https://thelexverse.com/speaker/

(4) https://about.facebook.com/

(5) https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/

(6) https://9to5mac.com/2022/07/17/everything-apple-ar-headset-mixed-reality/

(7) https://artificialintelligenceact.com/

à juste titre, être créé par la loi. Selon notre opinion, il n'est pas nécessaire de créer le concept de personne virtuelle ;

- un contrat virtuel conclu dans la réalité virtuelle aurait une force et un effet juridiques dans la plupart des pays. Toutefois, la détermination du lieu de conclusion de ce contrat pourrait poser des difficultés ;
- une signature virtuelle serait probablement qualifiée de signature électronique (8), un type de signature dont l'effet juridique est désormais reconnu par la plupart des pays ;
- une preuve virtuelle serait une forme de preuve électronique (9). De nombreux pays ont ou sont d'ailleurs en passe d'actualiser leurs législations en matière de preuves électroniques ;
- une infraction commise dans la réalité virtuelle relèverait de la cybercriminalité (10), dont la répression est déjà assurée par des lois existantes ;
- les entreprises peuvent d'ores et déjà être administrées virtuellement (11). Par exemple, les lois de nombreux pays permettent la tenue d'une réunion du conseil d'administration en réalité virtuelle.

▪ **Vie privée et réalité virtuelle.** Votre vie privée est-elle garantie dans la réalité virtuelle ? Quelqu'un peut-il y écouter vos conversations ? La législation sur la protection des données s'applique à la réalité virtuelle comme elle s'applique à toute forme de traitement des données à caractère personnel. La législation sur la protection des données est, en effet, fondée sur des principes et est technologiquement neutre, par conséquent, elle s'applique tout naturellement au monde virtuel. Quoi qu'il en soit, le degré du caractère privé et sécurisé d'un monde virtuel dépend du propriétaire de ce monde et il vous incombe donc d'être vigilant et de vérifier les politiques de confidentialité applicables à chacun des mondes virtuels auxquels vous participerez.

▪ **Sécurité et réalité numérique.** D'un côté, évoluer dans la réalité numérique est assez sécurisé. Les fournisseurs de casques virtuels ont intégré de nombreuses fonctions de sécurité dans leurs produits, et vous pouvez vous protéger davantage en vous fixant des limites virtuelles et en évitant de vous couper totalement du monde réel.

▪ D'un autre côté, la réalité virtuelle n'est pas à l'abri de la délinquance. Pour preuve, récemment, un avatar féminin a été agressée sexuellement. Vous pouvez également être exposé à des contenus illégaux ou préjudiciables dans la réalité virtuelle. La réalité virtuelle n'est donc ni sans danger ni exempte de criminalité :

- un délinquant peut voler les biens virtuels ou incorporels d'une autre personne ;
- un fraudeur peut escroquer quelqu'un dans la réalité virtuelle (cyberfraude) ;
- un harceleur peut intimider virtuellement sa victime, tout comme il le fait dans le monde réel ou cybernétique.

(8) https://www.michalsons.com/focus-areas/electronic-signature-law

(9) https://www.michalsons.com/focus-areas/information-technology-law/electronic-evidence-in-criminal-and-civil-proceedings

(10) https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world

(11) https://www.michalsons.com/blog/implement-the-companies-act-electronically/2565

▪ Les lois existantes, ainsi que les conditions d'utilisation définies par les propriétaires des différents mondes virtuels, sont dès lors indispensables pour assurer la sécurité des personnes lorsqu'elles se trouvent dans la réalité virtuelle par avatar interposé.

▪ **Protection de la propriété intellectuelle et réalité virtuelle.** Un enjeu majeur sera de savoir qui détient les droits sur la propriété virtuelle ou intellectuelle créée dans la réalité virtuelle. Les problématiques soulevées sont multiples et variées :

- Qui sera propriétaire du métavers, du monde virtuel en lui-même ?
- Sachant que des produits peuvent être produits en masse dans la réalité virtuelle, comment fonctionneront exactement les licences de marque dans ce contexte ?
- Qui sera propriétaire des contenus (NFT, mèmes, schémas, dessins, chansons, images etc.) créés dans la réalité virtuelle ?
- Une personne réelle pourra-t-elle faire valoir ses droits de la personnalité (droit à l'image) dans la réalité virtuelle ? Que se passera-t-il, par exemple, si quelqu'un crée un avatar qui vous ressemble ?

▪ **Protection des consommateurs.** De nouveau, une kyrielle de questions se surgissent : Les lois sur la protection des consommateurs s'appliquent-elles à la réalité virtuelle ? Oui, en grande partie, mais les législateurs devront peut-être être amenés à les adapter. Comment les entreprises diffuseront-elles des informations ou de la publicité dans le monde virtuel ? Quelles seront les modalités pour mettre en jeu la responsabilité d'une entreprise en cas de problème lié à la vente de biens ou de services virtuels ? Les délais de rétractation qui s'appliquent au commerce électronique s'appliqueront-ils également à la réalité virtuelle ? Pour cette dernière question, la réponse est probablement positive.

▪ **Plan d'action :**

- faites l'expérience d'une réunion virtuelle en demandant à nous rencontrer dans nos bureaux virtuels, en participant à nos webinaires ou en visionnant notre dernier webinaire ;
- sensibiliser les personnes concernées de votre organisation aux aspects juridiques de la réalité virtuelle en nous demandant d'organiser une formation sur ces thèmes qui vous est spécialement dédiée ;
- protégez vos droits dans la réalité virtuelle en sollicitant nos conseils sur le droit applicable à la réalité virtuelle.

JOHN GILES

south-africa@lexing.network

REFERENCES

The Lexverse Conference

▪ *On 8 June 2022 Michalsons hosted our first Lexverse Conference in South Africa. The legal universe about digital, data and emerging technologies. It was a chance for people to connect and interact, brainstorm and collaborate, discover something new and of course, look to the future. It was a hybrid event with people attending in person and online from virtually anywhere.*

▪ *The conference brought together globally recognised, visionary legal thought leaders, to discuss emerging technologies (like AI, the metaverse, blockchain and virtual reality) and their possible and existing regulations.*

▪ *Conference speakers included John Giles (managing attorney of Michalsons), Mike Abel (Founder & Chief Executive of M&C Saatchi Abel), Alain Bensoussan and Frédéric Forster (Lexing Alain Bensoussan Advocates) to name a few.*

Virtual reality law and regulation

▪ *We have recently spent time living in virtual reality and part of that is exploring the legal or regulatory aspects. Virtual reality law and regulation is a developing area of law.*

▪ ***Michalsons now has virtual offices.*** *Michalsons now has virtual offices and we try to meet in virtual reality whenever we can. Please contact us if you'd like to meet in our virtual offices. There are pros and cons to real, online or virtual meetings. It's important to pick the right type of meeting for the interaction you want to have.*

▪ ***We'll live in a world of mixed reality.*** *We're headed towards a world of mixed reality, which will be on the spectrum with virtual on one side and real on the other side. Augmented reality (AR) and mixed reality (MR) come somewhere in the middle. There are clear signals that we are moving into a world of mixed reality. For example, Facebook has re-banded Meta. Microsoft has acquired Activision and Apple is soon to launch its headset.*

▪ ***Virtual reality law and regulation.*** *Are there virtual laws? What laws apply in the virtual world? How are we going to regulate digital reality? These are all the important questions that we need to find answers to pretty quickly.*

▪ *There isn't currently a Virtual Reality Act (like the Artificial Intelligence Act) and we doubt that they ever will be. This is largely because existing laws are often drafted to be technology agnostic and principal based in a way which makes them applicable to the virtual world. In addition to the existing laws that apply, the owners of virtual worlds often draft terms and policies that would apply to anyone living in their virtual world. Let us look at a few examples of how existing laws would be applied in virtual reality:*

- *An avatar is probably a natural person under existing laws and not a juristic person. It also wouldn't be a robot person which is really a new kind of person the law needs to introduce. We don't believe it's necessary to create the concept of a virtual person;*

(1) https://thelexverse.com/

(2) Lexvers Conference 2022 Infographic

(3) https://thelexverse.com/speaker/

(4) https://about.facebook.com/

(5) https://news.microsoft.com/2022/01/18/microsoft-to-acquire-activision-blizzard-to-bring-the-joy-and-community-of-gaming-to-everyone-across-every-device/

(6) https://9to5mac.com/2022/07/17/everything-apple-ar-headset-mixed-reality/

(7) https://artificialintelligenceact.com/

- *A virtual contract concluded in virtual reality would be with legal force and effect in most jurisdictions. However, the place where the contract is concluded could pose difficulties.*
- *A virtual signature probably would be a form of electronic signature that most jurisdictions recognise as having legal effect.*
- *Virtual evidence would be a form of electronic evidence. Many countries are trying to update the laws to apply more specifically to electronic evidence.*
- *A crime committed in virtual reality would be the type of cybercrime and therefore any cyber crimes would apply and people could be convicted of those crimes under existing laws.*
- *It is possible to administer companies in virtual reality. For example, the laws of many countries enable a board meeting to be held in virtual reality.*

▪ ***Privacy and security in virtual reality.*** *How private and secure is virtual reality? Could somebody be listening in to my conversation? Data protection law applies to virtual reality as it applies to any form of processing personal data. Data protection law is principle-based and technology agnostic and therefore applies quite well in a virtual world. Virtual reality is only as private and secure as the owner of the world makes it. It is therefore very important to check the policies and the terms of the owner of the world.*

▪ ***How safe is digital reality?*** *It is pretty safe for the real person. The providers of headsets have built many great safety features into the products. People can keep themselves safe by setting virtual boundaries and by being able to look through the headset at the real world.*

▪ *But people can suffer harm whilst they're in virtual reality. Recently a female avatar has been sexually assaulted and it is possible that a person would be exposed to illegal or harmful material whilst in virtual reality. People can commit crimes against other people in virtual reality.*

- *Someone could steal someone else's virtual or incorporeal property.*
- *A fraudster could also defraud somebody in virtual reality – virtual fraud is an example of cyber fraud.*
- *A bully can virtually bully their victim much like they can in the real or cyber world.*

▪ *Both existing laws and the owner of the world, through the terms and policies, play a vital role in keeping people safe whilst they are in virtual reality represented by their avatar.*

▪ ***Intellectual property rights will be critical.*** *A critical issue will be who owns the rights to virtual or intellectual property created in virtual reality.*

- *Who will own the metaverse – the virtual world itself.*

(8) https://www.michalsons.com/focus-areas/electronic-signature-law

(9) https://www.michalsons.com/focus-areas/information-technology-law/electronic-evidence-in-criminal-and-civil-proceedings

(10) https://www.michalsons.com/focus-areas/cybercrime-law-around-the-world

(11) https://www.michalsons.com/blog/implement-the-companies-act-electronically/2565

- *How will brand licensing work? There is certainly a massive brand opportunity in virtual reality. Virtual products can be mass produced like never before.*
- *Who will own the content created in virtual reality – think NFTs, memes, diagrams, drawings, songs or images.*
- *Will real people be able to enforce their personality rights (aka publicity rights) in virtual reality? What if someone else creates an avatar that looks like them?*

▪ *Do consumer protection laws apply in virtual reality? Almost certainly yes, but lawmakers might need to adapt them. How will companies deliver information or advertising in the virtual world? How will people hold a business accountable for the sale of virtual goods or services? Will the cooling-off periods that apply to e-commerce also apply in virtual reality? Probably yes.*

▪ *Actions you can take:*

- *Experience a virtual meeting by asking to meet with us in our virtual offices, by attending one of our live public webinars or by asking us for a recording of our last webinar.*
- *Help the relevant people in your organisation consider the legal aspects of living in virtual reality by asking for us to conduct a private workshop for your organisation.*
- *Protect your rights in virtual reality by asking for our advice about virtual reality law.*

JOHN GILES

south-africa@lexing.network

REFERENCES

IA et la protection des données en Australie : état des lieux et actualités

Le changement de gouvernement pourrait-il freiner la position de l'Australie en faveur de l'IA et de la prise de décision automatisée ?

▪ Le récent changement de gouvernement en Australie va certainement avoir des répercussions dans ce domaine. Il sera particulièrement intéressant de suivre si, et dans quelle mesure, le nouveau gouvernement travailliste va s'engager en faveur de l'intelligence artificielle (IA) et la prise de décision automatisée. Pour rappel, l'ancien gouvernement de coalition avait publié une stratégie pour l'économie numérique dans le budget 2021-2022 **(1)**. Cette stratégie avait pour ambition de faire de l'Australie l'une des dix premières économies et sociétés numériques d'ici 2030. Cette stratégie tablait sur le fait que l'IA devait apporter plus de 20 000 milliards de dollars à l'économie mondiale d'ici à 2030 et créer potentiellement 1,2 million de nouveaux emplois dans le secteur des technologies en Australie d'ici à 2034.

▪ Alors que le nouveau gouvernement travailliste trouve ses marques, il ne fait aucun doute qu'il portera un regard critique sur l'actuelle stratégie pour l'économie numérique, et il est fort probable que de nombreux projets seront retravaillés, actualisés ou supprimés. On peut toutefois affirmer sans risque de se tromper que, quel que soit le bord politique auquel on appartient, l'IA et les technologies connexes joueront un rôle important pour le futur de l'Australie.

▪ Si on laisse de côté les changements politiques récents, le positionnement de l'Australie en tant que leader et précurseur de l'IA et de la prise de décision automatisée, va dépendre de la façon dont le pays va réussir à encadrer juridiquement l'économie numérique à mesure que les nouvelles technologies deviennent plus avancées et plus répandues. Comme toujours, le droit ne peut pas suivre le rythme de l'innovation numérique. La modernisation des cadres juridiques et des réglementations vise à renforcer la confiance du public à l'égard des nouvelles technologies, à mieux cerner leur utilisation et leurs avantages, à atténuer les risques et, en fin de compte, à encourager l'adoption accrue de technologies et à accroître les investissements dans l'économie numérique australienne.

▪ En mars 2022, le groupe de travail sur les technologies numériques a publié un document d'orientation intitulé « *Positioning Australia as a leader in digital economy regulation* » **(2)**, visant à placer l'Australie en position de leader en matière de réglementation de l'économie numérique. Dans ce cadre, deux axes majeurs ont été identifiés : l'IA et la prise de décision automatisée.

Qu'est-ce que l'IA et la prise de décision automatisée ?

▪ L'IA désigne un ensemble de technologies interdépendantes qui peuvent être utilisées pour résoudre des problèmes ou exécuter des tâches de manière

(1) https://digitaleconomy.pmc.gov.au/

(2) https://www.pmc.gov.au/domestic-policy/digital-technology-taskforce/positioning-australia-leader-digital-economy-regulation-automated-decision-making-ai-regulation

autonome, dans certains cas sans interaction humaine. L'IA a la capacité d'apprendre, de prédire et de prendre des mesures indépendantes.

▪ La prise de décision automatisée désigne, quant à elle, une technologie utilisée pour automatiser un processus de prise de décision. Elle implique souvent l'utilisation de formules basées sur des règles ou des algorithmes prédictifs.

▪ On observe des progrès rapides en matière d'IA et de prise de décision automatisée, que ce soit en Australie ou à l'étranger. L'IA permet par exemple à des camions autonomes de transporter en toute sécurité du minerai de fer vers des trains sans conducteur, à destination des ports d'Australie occidentale et d'autres marchés. La prise de décision automatisée est, elle, utilisée principalement dans les secteurs de la finance et de l'assurance, où elle aide au traitement des dossiers de demande de nouvelles polices d'assurance et de nouveaux comptes bancaires.

Nouvelles opportunités

▪ Le document d'orientation « *Positioning Australia as a leader in digital economy regulation* » souligne également les vastes possibilités qu'offrent l'IA et la prise de décision automatisée pour nos vies professionnelle et personnelle. En effet, ces nouvelles technologies sont susceptibles de stimuler la productivité, d'améliorer la prestation de services et de contribuer à résoudre un certain nombre de problèmes concrets.

▪ La stratégie pour l'économie numérique précitée met, pour sa part, en exergue le fait que la réduction des coûts de production et de livraison des biens et services entraînera une baisse des prix et des taxes. Elle met aussi en avant les avantages environnementaux et la possibilité pour les humains de se concentrer sur des tâches plus complexes et à haut risque grâce à la prise en charge par l'IA et la prise de décision automatisée des processus de routine.

▪ Outre les brefs exemples mentionnés ci-dessus, l'IA et la prise de décision automatisée en Australie sont déjà présentes dans presque toutes les industries et tous les secteurs. Notamment, l'IA est utilisée :

- dans le domaine médical, pour mesurer les mouvements d'un patient afin de détecter et de surveiller des maladies ou des affections (anévrisme cérébral, par exemple) ;
- dans le secteur de l'environnement, pour permettre le tri autonome de matériaux recyclés ;
- dans l'agriculture, pour cartographier les bourgeons, les fleurs et le nombre de fruits en vue d'améliorer la gestion des cultures ;
- dans le domaine fiscal, pour automatiser les déclarations de revenus afin de réduire les délais d'exécution ; et
- pour le service à la clientèle et les contrôles de sécurité, notamment les contrôles de passeports biométriques automatisés utilisant la technologie « SmartGate » dans les aéroports australiens.

L'état de la réglementation

▪ Le cadre éthique pour l'intelligence artificielle en Australie, l'*Australian Artificial Intelligence Ethics Framework* (2019) **(3)** définit déjà un certain nombre de principes à suivre pendant le cycle de vie des systèmes d'IA. Ces principes, auxquels chacun peut souscrire de manière purement volontaire, s'articulent autour de grands thèmes, tels que le bien-être humain, sociétal et environnemental, la protection de la vie privée, les valeurs centrées sur l'humain et la responsabilité.

(3) https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework

▪ En parallèle, le guide des meilleures pratiques en matière de prise de décision automatisée (*Automated Decision Making Better Practices Guide*) (2019) définit des outils et une liste de contrôle pour aider à la conception et à la mise en œuvre de nouveaux systèmes automatisés. Ce guide aborde des thèmes tels que l'assurance qualité, la transparence et la responsabilité, ainsi que les modalités d'évaluation de l'adéquation des systèmes automatisés.

▪ D'autres textes trouvent également à s'appliquer en la matière, par exemple :

- les principes sur l'IA de l'OCDE/G20 (2019), qui promeuvent une utilisation de l'IA qui respecte les droits de l'homme et les valeurs démocratiques ;
- la loi sur la protection de la vie privée de 1988 (*Privacy Act 1988 (Cth)*) : sa révision par le ministère de la justice devrait comprendre une étude des conséquences de la prise de décision automatisée sur la protection de la vie privée. Les commentaires des parties prenantes sur le sujet font actuellement l'objet d'un examen. Le nouveau ministre de la justice, Mark Dreyfus, s'est engagé à procéder à des réformes radicales au cours du mandat du gouvernement travailliste ;
- le plan d'action sur l'IA *(AI Action Plan (2021))* : ce document expose la vision stratégique de l'Australie pour devenir un leader mondial de l'IA ;
- le plan directeur pour les technologies critiques *(Blueprint for Critical Technologies (2021))* : ce texte identifie les technologies critiques qui sont porteurs soit d'avantages soit de risques pour l'intérêt national de l'Australie. Il répertorie 63 technologies critiques pour l'intérêt national, au premier rang desquelles l'IA, les algorithmes et les accélérateurs de matériel. Ce plan fixe quatre objectifs, et parmi ceux-ci figure la promotion de l'Australie en tant que partenaire de confiance pour l'investissement et l'innovation, et la garantie d'un accès à des technologies critiques sûrs et rentables.

Enjeux de l'IA et de la prise de décision automatisée

▪ Le document d'orientation dresse la liste des principaux problèmes liés à l'IA et à la prise de décision automatisée qu'il est nécessaire de gérer pour permettre à l'Australie de réaliser son ambition de devenir un leader mondial dans ce domaine.

▪ Les problèmes ainsi identifiés sont les suivants :

- **le caractère complexe et incertain de la réglementation** : le chevauchement des différentes réglementations, l'absence de dispositions formulées de manière technologiquement neutre et

l'existence d'exigences de conformité parfois contradictoires sont considérés comme des freins majeurs à l'innovation et au développement des technologies. Le document d'orientation reconnaît que la législation australienne n'a pas évoluée au même rythme que l'industrie, laissant ainsi les développeurs dans la confusion quant à la façon dont ils pouvaient se conformer aux multiples réglementations sectorielles spécifiques, qui ne prennent pas en compte la fonctionnalité ou la nature des nouvelles technologies.

- confiance du public : le manque de compréhension du fonctionnement de l'IA et de la prise de décision automatisée peut freiner l'adoption des nouvelles technologies en Australie. Des actions de sensibilisation par le gouvernement et le secteur privé, ainsi que la mise en place d'une réglementation sur les aspects relatifs aux risques et à la responsabilité peuvent constituer des leviers susceptibles de renforcer la confiance des consommateurs à l'égard des nouvelles technologies.
- risque de biais et manque transparence : les consommateurs s'inquiètent beaucoup des risques de biais et de discrimination pouvant résulter du fait que l'IA et la prise de décision automatisée reflètent les opinions de leur programmeur. Pour atténuer ces craintes, il conviendrait de renforcer la transparence du processus de prise de décision et des résultats. Toutefois, compte tenu de la complexité des algorithmes utilisés, et de la propriété intellectuelle et des informations confidentielles contenues dans ces technologies, des doutes existent quant à la faisabilité pratique d'assurer cette transparence et à la volonté des développeurs de dissiper cette opacité en divulguant le fonctionnement technique de leurs produits intégrant ces technologies.
- intervention humaine : le manque d'intervention humaine et l'impossibilité à faire preuve de jugement pour des cas spécifiques nécessitant une réponse personnalité et adaptées sont des reproches fréquemment formulés à l'égard de l'IA et de la prise de décision automatisée. Le document d'orientation souligne que si les nouvelles technologies qui appliquent des règles sans nécessiter de discrétion peuvent être plus simples à encadrer, ce n'est pas le cas de l'IA et la prise de décision automatisée qui impliquent une prise de décision discrétionnaire. Qu'en est-il, par exemple, des décisions relatives à l'octroi d'un prêt, à l'attribution d'un emploi ou à l'acceptation d'une demande pour obtenir le statut d'immigrant. La mise en balance entre, d'une part, l'efficacité qui peut être obtenue grâce l'IA et la prise de décision automatisée et, d'autre part, l'équité du résultat en raison de l'absence de décision discrétionnaire humaine méritent une attention particulière.
- vie privée : les technologies utilisant l'IA et la prise de décision automatisée peuvent inclure la collecte, l'examen et le regroupement de données personnelles (par exemple, des données d'identification, dont des données biométriques, des données financières ou encore des données de santé) provenant de diverses sources. Même si la loi sur la protection de la vie privée de 1988 s'applique bien à ces technologies, on

se demande si une réglementation supplémentaire pourrait être nécessaire pour faire face aux complexités liées à ces technologies.

Prochaines étapes

- Dans l'optique que l'Australie devienne une économie numérique mondiale d'ici à 2030, la stratégie pour l'économie numérique a jeté les bases pour favoriser la croissance, renforcer l'équipement en nouvelles technologies et concrétiser les ambitions affichées par des partenariats et des investissements stratégiques.

- Le nouveau gouvernement travailliste, dont l'agenda est déjà fortement chargé, prendra-t-il le relais en appliquant cette stratégie pour l'économie numérique, élaborée sous le gouvernement précédent ? Les premiers signes sont positifs. Le ministre de la justice, Mark Dreyfus, semble vouloir reprendre là où il s'est arrêté précédemment en 2013, alors qu'il occupait déjà ce poste. Ont ainsi été annoncées la possible création d'un nouveau délit civil pour les atteintes graves à la vie privée ainsi que la publication de propositions de réformes de la législation en matière de la vie privée. Reste à savoir si cela se traduira par une réforme politique substantielle et par les investissements nécessaires pour encourager, inciter et financer l'innovation numérique, et notamment l'IA et la prise de décision automatisée. Espérons que des mesures seront bientôt prises en ce sens, faute de quoi l'Australie risque de rater le train de l'IA et de la prise de décision automatisée qui, lui, n'attendra pas.

DUDLEY KNELLER

australia@
lexing.network

REFERENCES

AI and data protection in Australia – recent developments

A change in Government may put the brakes on Australia's support of AI and ADM? Or perhaps not?

▪ *The recent change to Australia's Government will likely see a raft of changes. Of particular interest is whether and to what extent the new Labour government will embrace artificial intelligence or AI and automated decision making or ADM. You will recall the release of the former Coalition government's Digital Economy Strategy in Budget 2021-2022* ***(1)****. The Strategy set a vision for Australia to be a top 10 digital economy and society by 2030. With AI projected to contribute more than $20 trillion dollars to the global economy by 2030 and provide a potential 1.2 million new technology jobs in Australia by 2034, the Strategy firmly turned its focus to the opportunities and benefits of AI and ADM in Australia.*

▪ *As the new Labour Government finds its feet, no doubt it will bring a critical lens to the existing Digital Economy Strategy with a good chance many of the proposed initiatives will be re-worked, updated or removed altogether. It is safe to say however that no matter which side of politics you are from there is no denying that support for AI and related technologies will feature strongly in Australia's future.*

▪ *Leaving aside current political dynamics, as part of positioning Australia as a leader and early adopter of AI and ADM, there has been a focus on how Australia will regulate a digital economy as new technologies become more advanced and widespread. As is always been the case the law and policy regulation cannot keep up with digital innovation. Modernising the legal frameworks and regulations is aimed at enhancing public trust and confidence around new technologies, increasing certainty around their use and benefits, mitigating risks and ultimately encouraging the increased adoption of technologies and investment in Australia's digital economy.*

▪ *In March 2022, the Digital Technology Taskforce issued the Issues Paper - Positioning Australia as a leader in digital economy regulation* ***(2)****, with a focus on AI and ADM.*

What is AI and ADM?

▪ *AI refers to a collection of interrelated technologies that can be used to solve problems or perform tasks autonomously, in some cases without human interaction. AI has the ability to learn, predict and take independent actions.*

▪ *ADM refers to technology that is used to automate a decision making process. This often involves the use of rule based formulas or predictive algorithms.*

▪ *Both AI and ADM are advancing quickly in Australia and overseas. AI works hard to ensure autonomous trucks safely transport iron ore to waiting driverless trains bound for Western Australian ports and waiting markets. ADM has gained enormous popularity in the financial and insurance sectors, helping to vet applications for new policies and accounts.*

(1) https://digitaleconomy.pmc.gov.au/

(2) https://www.pmc.gov.au/domestic-policy/digital-technology-taskforce/positioning-australia-leader-digital-economy-regulation-automated-decision-making-ai-regulation

New Opportunities

▪ *The Issues Paper emphasises the vast opportunities presented by AI and ADM to our work and personal lives. These new technologies are considered to boost productivity, improve service delivery and help solve a number of real-world problems.*

▪ *The Strategy has stated that the reduction in the costs of producing and delivery goods and services will lead to lower prices and lower taxes. Environmental benefits and the ability for humans to focus on more complex and high risks tasks due to the use of AI/ADM for routine processes are also highlighted as benefits of this new technology.*

▪ *In addition to the brief examples noted above, the use of AI and ADM in Australia already spans across nearly every industry and sector, including:*

- *the use of AI in the medical industry to measure a patients range of motions to detect and monitor conditions such as brain aneurysm;*
- *use of AI to allow the autonomous sorting of recycled materials;*
- *the use of AI in agriculture to map buds, flowers and fruit counts to improve management of crops;*
- *the use of ADM to automate tax returns to reduce turnaround; and*
- *the use of ADM for customer service and security checks, including the biometric passport checks automated through SmartGate at Australian airports.*

The state of regulation

▪ *The existing Australian Artificial Intelligence Ethic's Framework (2019)* ***(3)*** *already sets out a number of principles to follow during the AI system lifecycle. These principles are voluntary and include consideration of factors including human, societal and environmental wellbeing, privacy protection, human-centred values and accountability.*

(3) https://www.industry.gov.au/data-and-publications/australias-artificial-intelligence-ethics-framework

▪ *Similarly, the Automated Decision Making Better Practices Guide (2019) sets out tools and a checklist to assist in designing and implementing new automated systems. The guidance includes areas such as quality assurance processes, transparency and accountability and assessing the suitability of automated systems.*

▪ *Other regulations that currently apply to new technologies include:*

- *OECD/G20 AI Principles (2019) – which promotes the use of AI that also respects human rights and democratic values.*
- *Privacy Act 1988 (Cth) – the current review of the Privacy Act by the Attorney General's Department is set to include an examination of the privacy implications of ADM with a discussion paper currently considering feedback from stakeholders. New Attorney General Mark Dreyfus has committed to "sweeping reforms" during Labour's first term in office.*

- *AI Action Plan (2021) – Australia's strategic vision to become a global leader in AI.*
- *Blueprint for Critical Technologies (2021) – identifies critical technologies that have the capacity to enhance or pose a risk to Australia's national interest. The Blueprint includes 63 critical technologies for the national interest including AI, algorithm and hardware accelerators. The blueprint includes four goals including promoting Australia as a trusted and secure partner for investment and innovation and ensuring there is access to critical technologies that are secure and cost efficient.*

Issues and concerns with AI/ADM

▪ *The Issue Paper outlines the key issues relating to AI and ADM which need to be addressed to enable Australia to succeed in its vision of becoming a global leader in this space.*

▪ *The critical issues outlined in the Issues Paper include:*

- *Regulatory uncertainty and complexity – overlapping regulations, the lack of technology neutral language and contradictory compliance requirements are seen as a major deterrence to innovation and the development of technologies. The Issues Paper acknowledges that Australian regulators have been perceived as lagging behind industry in responding to new technologies, leaving developers confused regarding how they can comply with multiple sector specific regulations that do not take into account the functionality or nature of new technologies.*
- *Public trust and confidence – a lack of understanding regarding how AI and ADM works is seen as a potential barrier to the uptake of new technologies in Australia. Education by the Government and private sector as well as regulation regarding risk and liability are seen as ways to provide consumers with greater certainty regarding the use of new technologies.*
- *Potential for bias and transparency – a significant concern for consumers is the potential for bias and discrimination as a result of the AI/ADM reflecting the views of their programmer. Transparency in the decision making process and outcomes is seen as an option of addressing this concern. Given the complexity of algorithms used and the intellectual property and confidential information contained in technologies, there are issues regarding the practicalities and willingness of developers to divulge technical workings of their AI/ADM products.*
- *Discretion – the lack of human discretion and inability to make judgment calls for bespoke scenarios is a common criticism of AI/ADM. The Issues Paper highlights that while new technologies that clearly follow a set of rules without the need for discretion may be simpler to regulate, AI and ADM which involves discretionary decision making may be more complicated. The granting of a loan, employment offer or immigration status are examples which bring this question to light. The balance between the efficiency which may be achieved through AI/ADM and the*

fairness of the outcome due to a lack of human discretional decision making is a topic which requires further public consideration.

- ***Privacy –*** *Technologies using AI and ADM may include the collection, examination and collation of personal information (e.g. identification information, including biometric information, financial information and health information) from various sources. While the Privacy Act 1988 applies to these technologies, there is concern regarding whether further regulation is required to address the complexities related to such technologies.*

So where to from here?

▪ *In order to meet Australia's vision of being a global digital economy by 2030, the Digital Economy Strategy intends to focus on policies that build the right foundations that enable growth, build capabilities in new technologies and lift ambition through collaboration and strategic investment.*

▪ *It is yet to be seen to what extent the new Labour government will pick up this baton, with already a full agenda of policy initiatives competing for attention. Early signs however are positive. As noted above the Attorney General, Mark Dreyfus seems to be keen to pick up where he left off in 2013. There is talk of a new tort for serious breaches of privacy and alike and he has also announced he will publish the proposed privacy reforms currently being considered. Whether this will translate into substantive policy reform and the necessary investment to encourage, incentivise and fund digital innovation, including AI and ADM is just not clear at this point. Let's hope there is clarity soon or Australia will be left behind at a critical juncture. Neither AI nor ADM innovation has the patience to wait.*

DUDLEY KNELLER

australia@
lexing.network

REFERENCES

Voitures autonomes et discrimination : les fournisseurs de systèmes d'IA entre le marteau et l'enclume

▪ « *Between the Hammer and the Anvil* », c'est-à-dire « entre le marteau et l'enclume », n'est pas seulement une grande chanson du groupe de heavy metal Judas Priest, c'est aussi la position périlleuse dans laquelle les fournisseurs de systèmes d'IA pourraient se retrouver dans quelques mois.

▪ Une multitude de facteurs fait que l'on arrivera prochainement à cette situation. Aujourd'hui, les véhicules autonomes gagnent, lentement mais sûrement, du terrain, et les constructeurs automobiles les équipent d'une assistance à la conduite de plus en plus sophistiquée. Le pilote automatique de Tesla a déjà atteint le niveau 2 du niveau d'automatisation de la conduite selon le classement établi par la *Society of Automotive Engineers* (SAE), et début 2022, Mercedes a même annoncé un niveau 3 pour ses modèles Classe S et EQS haut de gamme. Le niveau 3 correspond, rappelons-le, à une situation d'automatisation conditionnelle où le conducteur humain ne conduit que lorsque le système de conduite autonome du véhicule le lui demande, tout en étant tenu de rester vigilant.

▪ En parallèle, la législation évolue également. Ainsi, en janvier 2022, la Convention de Vienne sur la circulation routière a été modifiée de manière à ce que l'exigence, prévue par ce texte, selon laquelle tout véhicule en mouvement doit avoir un conducteur, soit réputée satisfaite lorsque le véhicule utilise un système de conduite automatisé conforme. Des règlements établis par les organismes compétents des Nations Unis (par exemple, les règlements ONU n°R155, R156 et 157 sur les systèmes automatisés de maintien dans la voie) et des Etats, vont venir préciser les détails de ces systèmes.

▪ Bien entendu, comme les véhicules autonomes sont truffés d'intelligence artificielle et traitent de grandes quantités de données, ils doivent se conformer aux réglementations en la matière. Dans l'Union européenne, les constructeurs automobiles devront donc probablement se conformer au futur règlement établissant des règles harmonisées concernant l'intelligence artificielle. « Probablement » car, à ce jour, cette proposition de règlement manque encore de clarté à ce sujet. En effet, ses articles 2 et 6 et son annexe II prêtent à confusion quant à leur application aux voitures autonomes qui intègrent des systèmes d'IA à haut risque utilisés en tant que composants de sécurité desdits véhicules. Ceci étant dit, même en cas de doute, il sera plus prudent d'appliquer les dispositions de ce futur règlement aux systèmes d'IA présents dans les véhicules autonomes, d'autant plus que ces systèmes d'IA sont considérés comme à haut risque.

▪ Parmi les exigences de conformité énoncées par la proposition de règlement de l'UE sur l'IA, l'article 10.4 est particulièrement intéressant car il prévoit que *« Les jeux de données d'entraînement, de validation et de test tiennent compte, dans la mesure requise par la destination, des caractéristiques ou éléments propres au contexte géographique, comportemental ou fonctionnel spécifique dans lequel le système d'IA à haut risque est destiné à être utilisé »*.

▪ Cette disposition peut toutefois s'avérer délicate à appliquer car, en termes de conduite automobile, comme pour de nombreuses activités humaines, les caractéristiques d'un comportement « normal » dépendent fortement du contexte.

Les différences de comportement au volant, sources de stéréotypes et de plaisanteries, ont été prouvées dans une certaine mesure par une expérience, baptisée la *Moral Machine*, menée par le MIT et le CNRS. Dans le cadre de cette expérience, des chercheurs ont interrogé les internautes afin de savoir comment ils résoudraient les dilemmes moraux auxquels sont confrontés les véhicules autonomes. Variante du célèbre dilemme du tramway, l'expérience consistait à demander aux internautes de choisir comment une voiture autonome devrait réagir dans diverses situations de conduite délicates (éviter trois enfants dans la rue mais tuer les passagers de la voiture, éviter une dame âgée mais tuer un chien...). L'expérience a permis aux chercheurs de récolter plus de 40 millions de réponses et les résultats, publiés dans la revue *Nature*, montrent que les choix moraux peuvent être très différents d'un pays à l'autre, même entre des pays géographiquement proches, tels que la France et la Belgique. L'expérience *Moral Machine* fait ainsi ressortir des différences régionales et culturelles notables dans les choix que doivent faire les systèmes de conduite autonome dans des situations critiques. Et ces différences se retrouveront forcément dans les différents jeux de données d'entraînement, de validation et de test, ainsi que dans les données d'entrée. Or, cela pourrait conduire à des « boucles de rétroaction », qui doivent justement faire l'objet de mesures d'atténuation, conformément à l'article 15 de la proposition de règlement sur l'IA.

(1) « Turbo Lover » et « Heading Out to the Highway »

- Dès lors, les questions affluent : ces différences peuvent-elles être qualifiées de biais ? Si oui, selon quelle norme ? Dans quelle mesure ces différences peuvent-elles/doivent-elles être intégrées dans les jeux de données ? En outre, pour appliquer ces différences, il se peut que le traitement des données à caractère personnel (homme/femme, jeune/vieux, personne malade/en bonne santé, personne sportive/avec une surcharge pondérale etc.) doive être effectué, à la volée, par le véhicule, ce qui déclencherait alors l'application du RGPD.

- De ce fait, les constructeurs risquent d'être pris entre différents intérêts contradictoires : la conformité aux règles de l'IA, la conformité au RGPD (et toutes autres règles en matière de lutte contre les discriminations) et, enfin et surtout, les attentes (changeantes) des consommateurs quant au comportement d'un véhicule autonome dans des situations critiques. Pour contourner cette difficulté, les constructeurs pourraient être tentés d'utiliser volontairement des technologies « aveugles » (par exemple, le LIDAR au lieu de la caméra) afin de ne pas enfreindre la loi et, surtout, d'échapper à tout soupçon de discrimination. La solution peut également reposer sur la doctrine du capitalisme (plus vous payez, plus vous êtes protégé) ou de celle de l'utilitarisme (seule la préservation de la majorité compte). Enfin, il est possible de déployer une « IA régionaliste », même si cela ne ferait que susciter davantage de questions quant à la segmentation du marché ou à l'apparition d'une boucle de rétroaction. A l'inverse, une « IA uniforme » pourrait effacer les particularités « locales », au risque toutefois d'établir l'hégémonie culturelle des principaux développeurs de ces systèmes d'IA.

- Pour l'instant, la situation décrite ci-dessus peut sembler relever de la science-fiction à tous les mangeurs d'asphalte, célébrés dans deux autres chansons de Judas Priest **(2)**, mais n'en reste pas moins intéressante, car l'avalanche de questions soulevées par le cas spécifique de la conduite automatisée au moyen de l'intelligence artificielle (biais, discrimination et hégémonie culturelle) pourrait bien se répéter pour d'autres types d'automatisation dans le futur.

ALEXANDRE CASSART

belgium@lexing.network

Autonomous cars and discrimination: IA systems providers between the hammer and the anvil

▪ *Between the Hammer and the Anvil isn't only a great song by Judas Priest, it is also the unfortunate position in which IA systems providers may find themselves in a few months.*

▪ *Various factors are slowly converging to get to this situation. Autonomous vehicles are—slowly but steadily—gaining traction. Car manufacturers are equipping their flagship's cars with more sophisticated driving assistance. Following the matrix of driving automation published by the Society of Automotive Engineers (SAE), the now widely spread Tesla's autopilot has already reached level 2. Beginning of 2022, for its high end Classe S and EQS, Mercedes has even announced a level 3 of driving automation. At level 3, the driver must stay alert, but it only has to drive when the system requests it.*

▪ *And the legislation evolves along with the business. In January 2022, the Vienna Convention on Road Traffic has been amended so that the driver's requirement—upon which the Convention is build—may be satisfied by the reliance on a compliant autonomous driving system. Various UN (e.g. UN R155, R156 and 157 on Automated Lane Keeping Systems) and national regulations will specify the details of said systems.*

▪ *Of course, autonomous vehicles relying heavily on artificial intelligence and data processing, they have to be compliant with relevant regulations. In the European Union, the car manufacturers will probably have to comply with the future regulation laying down harmonized rules on artificial intelligence. 'Probably' because the proposal lacks clarity on this so far. Art. 2, art. 6 and the Annex II are confusing as to the application of the regulation to autonomous cars involving high-risk AI Systems being safety components of said vehicles. That being said, it shall probably be a safe bet to apply the regulation to AI systems within autonomous vehicles, especially since such AI systems are deemed as high risk.*

▪ *Amongst the compliance requirements laid out by the proposal, Art. 10.4 is especially interesting as it provides that 'Training, validation and testing data sets shall take into account, to the extent required by the intended purpose, the characteristics or elements that are particular to the specific geographical, behavioural or functional setting within which the high-risk AI system is intended to be used.'*

▪ *This can prove to be tricky. Indeed, as with many human activities, driving style and expectations of a 'normal' behaviour are highly dependent on the context. This is fuelling stereotypes and jokes, but it has been proved to an extent by an experiment led by the MIT and the CNRS, the Moral Machine. A variation on the famous tramway dilemma, the experiment collected more than 40 million answers to various driving situations where the driver had to choose between bad occurrences (avoid three children on the street but killing the passengers of the car,*

avoid an elderly lady but killing a dog…). The results, published in Nature, demonstrate that decisions may be very different, even between countries that are close geographically, such as France and Belgium.

- *The Moral Machine experiment demonstrates marked regional and cultural differences in the choices that must be made by autonomous driving systems in critical situations. These differences will be marked in the different training, validation and test datasets, but also in the input data (which may lead to a feedback loop whose mitigation obligation is referred to in Article 15).*

- *This leads to various questions. Can these differences be characterized as bias? If so, against what standard? To what extent can/should these differences be incorporated into the datasets? In order to respect these differences, personal data processing may have to be carried out, on the fly, by the vehicle: Male/Female, Young/Old, Sick/Healthy, Sporty/Overweight… Which triggers the application of the GDPR to such data processing.*

- *Manufacturers risk being caught between conflicting interests, compliance with AI rules, compliance with the GDPR (and other anti-discrimination rules) and, last but not least, consumers' (shifting) expectations of how an autonomous vehicle should behave in critical situations. In order to avoid the difficulty, manufacturers may be tempted to voluntarily use 'blind' technologies (e.g. LIDAR instead of camera) so as to avoid breaking the law and, especially, evade any suspicion of discrimination. The solution may also be capitalistic (the more you pay, the more you are protected) or utilitarian (only the preservation of the majority counts). Finally, 'regionalist' AI may be deployed, which only generates more question as to market segmentation or the occurrence of a real-life feedback loop. To the contrary, 'uniform' AI may erase 'local' particularities and establish the cultural hegemony of the main developers of these AI systems.*

- *So far, the situation described above may sound like science fiction to all Turbo Lovers, Heading Out to the Highway, but the specific case of automated driving using artificial intelligence could be representative of other future automation, raising the same questions: biases, discrimination, cultural hegemony.*

ALEXANDRE CASSART

belgium@lexing.network

REFERENCES

Etude comparée des dispositions de la PIPL et du RGPD

▪ Le RGPD européen et la PIPL chinoise (« *Personal Information Protection Law* ») ont été publiés à plus de 5 ans d'intervalle **(1)**. Bien que de nombreuses clauses de la PIPL soient inspirées du RGPD et que la PIPL et le RGPD partagent de nombreux points communs, la PIPL reste néanmoins significativement différente du RGPD sur de nombreux aspects clés.

Terminologie

▪ Tout d'abord, avant toute chose, il convient de bien maîtriser la terminologie de la PIPL, qui peut inclure un certain nombre de faux amis. En effet, dans la version anglaise de la PIPL, le « *data processor* » **(2)** désigne « toute organisation ou personne qui détermine, de manière indépendante, la finalité et les moyens du traitement lors du traitement des informations personnelles ». Ainsi, le « *processor* » chinois correspond au « *controller* » européen (responsable du traitement), défini dans le RGPD **(3)** comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement, tandis le « *processor* » européen (sous-traitant ») correspond dans la version anglaise de la PIPL, à une « *entrusted party for data processing* » (c'est-à-dire à la partie en charge du traitement des données) **(4)**.

Champ d'application territorial

▪ La PIPL est l'une des rares lois chinoises à revendiquer une application extraterritoriale. De fait, la PIPL s'applique non seulement aux traitements de données personnelles effectués sur le territoire chinois, mais aussi aux traitements de données personnelles effectués par un responsable du traitement établi dans un pays étranger lorsque ceux-ci impliquent des personnes localisées sur le territoire chinois **(5)**. La PIPL est donc applicable à tous les traitements impliquant des personnes concernées se trouvant sur le territoire chinois. La PIPL se distingue en cela du champ d'application territorial du RGPD, qui dispose, quant à lui, que « le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. »

Base légale du traitement de données

▪ La PIPL prévoit que les données personnelles ne peuvent être traitées que sur le fondement de l'une des bases légales visées à son article 13. A noter que, contrairement à ce qui prévu à l'article 6.1 (f) du RGPD, ne constitue pas une base légale au titre de la PIPL les intérêts légitimes poursuivis par le responsable du traitement.

(1) Le RGPD, publié le 27 avril 2016, est entré en vigueur le 25 mai 2018. La loi sur la protection des informations personnelles de la RPC, publiée le 20 août 2021, est entrée en vigueur le 1er novembre 2021.

(2) PIPL, article 73.

(3) RGPD, article 4.

(4) PIPL, article 21.

(5) PIPL, article 3.

Informations à fournir avant tout traitement de données personnelles

▪ Dans la PIPL, le responsable du traitement est tenu de fournir certaines informations à la personne concernée. Ces informations doivent être présentées de façon bien visible, sous une forme compréhensible, et formulées en des termes clairs, de manière sincère, précise et complète (6). L'exigence de compréhensibilité signifie notamment que l'information donnée soit disponible en langue chinoise.

(6) PIPL, article 17.

▪ De son côté, le RGPD prévoit deux scénarios pour la fourniture d'informations aux personnes concernées, selon que les données personnelles sont collectées auprès de la personne concernée (article 13) ou non (article 14). Le RGPD et la PIPL divergent en ce qui concerne la liste des informations à fournir (la base juridique du traitement, les destinataires ou les catégories de destinataires des données à caractère personnel etc.).

Catégories particulières de données personnelles

▪ Dans la PIPL, les « informations personnelles sensibles » sont définies comme des « informations personnelles qui, si elles sont divulguées ou utilisées à des fins illégales, sont susceptibles de porter atteinte à la dignité/l'honneur d'une personne ou à la sécurité de sa personne/de ses biens ». Sont notamment qualifiées comme telles les données biométriques, les convictions religieuses, l'identité spécifique, les données concernant la santé, les informations relatives aux comptes ouverts auprès d'institutions financières, les données de géolocalisation et les données personnelles des mineurs de moins de 14 ans.

▪ Le RGPD interdit, pour sa part, le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. Selon le texte européen cette interdiction ne peut être levée que dans des cas limitativement énumérés à son article 9.2.

Transfert transfrontalier de données personnelles

▪ Aux termes de la PIPL, si cela est justifié par des raisons commerciales, un responsable du traitement peut procéder au transfert vers l'étranger de données personnelles sous réserve de remplir l'une des conditions légales prévues par le PIPL. Par ailleurs, il est interdit à un responsable du traitement de fournir des données personnelles stockées sur le territoire chinois à une autorité judiciaire étrangère ou à un organisme répressif étranger, sans avoir obtenu l'autorisation préalable des autorités chinoises compétentes.

▪ Par comparaison, le RGPD prévoit (7) un système plus complexe et à plusieurs niveaux pour le transfert de données hors de l'UE. En substance, l'une des conditions suivantes doit être remplie :

(7) RGPD, chapitre V.

- l'existence d'une décision d'adéquation adoptée par la Commission européenne ;
- la fourniture, par le responsable du traitement ou le sous-traitant, de garanties appropriées et à condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

Délégué à la protection des données

▪ En Chine, lorsque le nombre de traitements mis en œuvre atteint un certain seuil, le responsable du traitement est tenu de désigner une personne responsable de la protection des informations personnelles, et de porter les coordonnées de cette personne à la connaissance du public. Cette personne serait l'équivalent du délégué à la protection des données (DPO) institué par le RGPD.

▪ Toutefois, le DPO, tel que défini par le RGPD **(8)**, semble avoir un statut très différent vis-à-vis du responsable du traitement ou du sous-traitant qui l'emploie. Par exemple :

- le responsable du traitement et le sous-traitant veillent à ce que le DPO ne reçoive aucune instruction en ce qui concerne l'exercice des missions ;
- le DPO ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions ;
- le DPO fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.

(8) RGPD, articles 37-39.

Autorités en charge de la protection des données

▪ Dans le cadre de la PIPL, les autorités du cyberespace jouent le rôle de « coordinateur » pour les activités de protection et de surveillance des données entre les différents départements ministériels du gouvernement central. Le pouvoir de contrôle est donc décentralisé.

▪ Dans le cadre du RGPD, les autorités de contrôle semblent s'inscrire dans le cadre d'un pouvoir centralisé.

JUN YANG

china@
lexing.network

REFERENCES

Comparative review of key aspects of PIPL and GDPR

▪ *The GDPR and the Chinese PIPL ("Personal Information Protection Law") were released with more than 5 years apart.* ***(1)*** *Though many clauses of the PIPL are inspired by GDPR and PIPL and GDPR share many in common, PIPL remains nevertheless significantly different from GDPR in many key aspects.*

Terminology

▪ *When navigating the terminology of PIPL, we may come across a number of "false friends" of which the most notorious one is the Data Processor (Personal information processor). The term Data Processor (Personal information processor) used in PIPL* ***(2)*** *refers to "any organization or individual that independently determines the purpose and means of processing in their processing of personal information." It corresponds to the definition of "data controller" in GDPR ("natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data")* ***(3)*** *whilst "Entrusted party for data processing"* ***(4)*** *corresponds to the "processor" under GDPR.*

Territorial scope of application

▪ *PIPL is one of a few Chinese laws claiming extra-territorial application. The PIPL applies to not only the processing of personal information in Chinese territory but also that of personal information involving individuals in Chinese territory by a processor based in an overseas jurisdiction* ***(5)****. The underlying consideration for territorial application of PIPL is whether the data subjects in Chinese territory are concerned by the processing in question. This is obviously different from the territorial scope clause of GDPR which reads "this regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."*

Legal basis for data processing

▪ *Article 13 of PIPL provides that personal data may be processed only under any of the statutory circumstances specified therein. The processing based on "legitimate interests" under article 6.1 (f) of GDPR is not covered by PIPL.*

Information to be provided prior to the processing of personal data

▪ *The data controller shall inform the data subject concerned of the following in a distinguishable form and in intelligible and plain language and in a sincere,*

(1) GDPR was released on April 27, 2016 and took effect on August 25, 2018. The PRC Personal Information Protection Law was released on August 20, 2021 and became effective on November 1, 2021.

(2) PIPL, article 73.

(3) GDPR, article 4.

(4) PIPL, article 21.

(5) PIPL, article 3.

(6) PIPL, article 17.

accurate and complete fashion **(6)**. *The above requirement such as "intelligible language" implies in a Chinese context that the information should be available in Chinese language as well.*

▪ *GDPR addresses the information issue by its article 13 and 14 depending upon different scenarios: Information to be provided where personal data are collected from the data subject (article 13); information to be provided where personal data have not been obtained from the data subject (article 14). There are also a number of differences between GDPR and PIPL regarding the scope of the information such as the "legal basis", "recipients or categories of recipients of the personal data"*

Special categories of personal information

▪ *"Sensitive personal information" refers to "personal information which, if disclosed or used for illegal purpose, is likely to undermine the dignity/honor of an individual or expose his/her personal safety/property to danger, including biometrics, religious belief, specific identity, health, accounts opened with financial institutions, itinerary tracking and personal information of a minor under the age of 14 years."*

▪ *GDPR prohibits processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and the processing of genetic data, biometrics data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. Such prohibition shall be lifted only in a limited number of circumstances specified in article 9.2 of the GDPR.*

Outbound transfer of personal data

▪ *A processor, if justified by a business reason, may proceed with outbound transfer of personal information if one of the statutory conditions is fulfilled under PIPL. Processor shall be prohibited from providing personal information stored in Chinese territory to any foreign judiciary or law enforcement department unless duly approved by Chinese competent authorities.*

▪ *GDPR provides a more complex and tiered system for the international data transfer* **(7)**, *basically, the international data transfer shall bear one of the following basis:*

- *An adequacy decision rendered by EU commission;*
- *The data controller or processor has provided appropriate safeguards and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.*

(7) GDPR, chapitre V.

Person in charge of Data Protection

▪ *A processor whose processing attaining the quantitative threshold shall appoint a person responsible for personal information protection and the contact details of*

this person shall be made known to the public. This "person responsible for personal information protection" is seemingly the equivalent to the "Data protection officer" under GDPR.

▪ *The DPO defined by GDPR* ***(8)*** *appears to have a very different status vis-à-vis the data controller/processor employing the DPO, to just quote the following:*

- *the controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of his/her tasks.*
- *He or she shall not be dismissed or penalized by the controller or the processor for performing his task.*
- *The DPO shall directly report to the highest management level of the controller/processor.*

(8) GDPR, articles 37-39.

The authorities in charge of data protection

▪ *Under PIPL, Cyber-Space authorities remain as the « coordinator » for the data protection and supervisory activities among different ministerial departments under the central government. The supervisory power is therefore decentralized.*

▪ *Supervisory authorities appear to have centralized power under GDPR.*

JUN YANG

china@
lexing.network

ESPAGNE

LEXING SPAIN

Retour sur la conférence espagnole régionale sur le métavers

▪ Le 9 juin 2022, le lendemain de la conférence mondiale Lexing, au cours de laquelle le cabinet Lexing Spain est intervenu sur le thème de la réglementation du métavers au niveau européen, nous avons organisé un webinaire en espagnol sur le même thème, depuis notre propre bureau virtuel dans le métavers, pour aborder cette question sous un angle à la fois juridique et commercial.

▪ Dans la première partie du webinaire, deux consultants experts dans le domaine de la transformation numérique et des technologies de réalité virtuelle et augmentée sont intervenus pour partager leur expertise et expliquer ce qu'est le métavers, l'état actuel de son développement et les technologies qui y sont associées. Ils ont ensuite donné une série de lignes directrices et de recommandations aux entreprises qui souhaitaient lancer un projet dans le métavers. La recommandation la plus importante à cet égard est que les entreprises doivent commencent à expérimenter ce nouvel environnement pour mieux comprendre les opportunités commerciales que le métavers peut leur offrir.

▪ La deuxième partie du webinaire était consacrée plus particulièrement aux risques juridiques posés par le métavers et aux différentes manières de les gérer avec le cadre juridique existant. A cette occasion, ont été passés en revue les thématiques pouvant avoir un impact sur les projets dans le métavers, tels que la protection de la vie privée et des données, la création et la vente de NFT, la protection de la propriété industrielle et intellectuelle, et la résolution des conflits. Le webinaire s'est terminé par le constat qu'il sera nécessaire d'envisager de réformer le droit actuel pour tenir compte des spécificités du métavers pour lesquelles la réglementation actuelle n'apporte pas de réponses adéquates.

▪ Enfin, ce webinaire s'est conclu par une session de questions et réponses.

▪ Le contenu complet de webinaire est accessible en ligne **(1)**.

REFERENCES

(1) Webinar EL METAVERSO, ¿MUCHO RUIDO Y POCAS NUECES : https://www.youtube.com/watch?v=RcPZvIQwhjI&feature=youtu.be

MARC GALLARDO

spain
@lexing.network

Spanish Local Metaverse Conference Review

▪ *On 9 June 2022, the day after the Lexing global conference, where we had the opportunity to talk about the regulation of the metaverse at EU level, we held a webinar in Spanish on the same topic of the Metaverse and from our own virtual office in the Metaverse, with a business and legal approach.*

▪ *In the first part of the webinar, we had the participation of two prominent consultants in digital transformation and virtual and augmented reality technologies, who explained what is meant by Metaverse, the current state of its development and the technologies that are involved in it, to then give a series of guidelines or recommendations to companies that want to start some kind of project in the Metaverse. The most important recommendation in this regard is for companies to start experimenting in this new environment to better understand the business opportunities that the Metaverse can offer them.*

▪ *The second part of the webinar addressed the legal risks that the Metaverse poses and how to deal with them within the existing legal framework, mentioning more specific aspects that impact on projects in the Metaverse such as privacy and data protection, the creation and sale of NFT's, protection of industrial and intellectual property, and conflict resolution in the Metaverse. The most salient conclusion is that it will be necessary to consider reforming current law to accommodate specific situations in the Metaverse for which current regulation does not have adequate answers.*

▪ *At the end of this presentation, a question and answer session was opened.*

▪ *The webinar was well attended and the full content of the webinar is available online* ***(1)****.*

REFERENCES

(1) Webinar EL METAVERSO, ¿MUCHO RUIDO Y POCAS NUECES: https://www.youtube.com/watch?v=RcPZvIQwhjI&feature=youtu.be

MARC GALLARDO

spain
@lexing.network

Métavers : Quelle réglementation aux USA ?

▪ Le mot « métavers » est constitué de la contraction du préfixe grec « meta » signifiant « au-delà », et de « univers ». Le métavers est donc un monde qui va « au-delà de notre univers ». Issu de la science-fiction, le concept de métavers est apparu pour la première fois en 1992 dans le roman « Snow Crash » (traduit en français sous le titre « Le Samouraï virtuel ») de Neal Stephenson, où il désigne un univers virtuel contrôlé et détenu par un « monopole mondial de l'information auquel les utilisateurs peuvent accéder via des lunettes de réalité virtuelle personnelles ». A l'heure actuelle, le métavers est encore à l'état embryonnaire et il n'existe pas véritablement d'endroit unique qui constituerait « le » métavers, mais bien de nombreux mondes virtuels alimentés par une série d'innovations technologiques, créant de ce fait des questions juridiques inédites.

▪ Le métavers incarne l'évolution d'internet vers « un monde virtuel unique, universel et immersif, grâce à l'utilisation de casques de réalité virtuelle (RV) et de réalité augmentée (RA) ». **(1)** L'immersion totale dans le métavers passe également par d'autres accessoires haptiques, c'est-à-dire qui stimulent le sens du toucher et du mouvement, tels que des combinaisons ou même des nunchakus.

▪ L'ambition du métavers : donner vie au monde virtuel ! Ainsi, nous pourrons, en prenant la forme d'un avatar, exister dans un espace virtuel 3D et y réaliser la plupart des choses que nous faisons dans le monde « réel » : faire du shopping, suivre des cours, travailler, assister à des concerts, faire du sport, participer à des événements sportifs, ou encore posséder des biens et faire des investissements créatifs et financiers à des fins lucratives.

▪ Le métavers attise toutes les convoitises et les entreprises cherchent naturellement à en tirer profit. Par exemple, Facebook a rebaptisé sa société mère « Meta » et investi 180 milliards de dollars pour développer le métavers. Son PDG, Mark Zuckerberg, a déclaré qu'il était plausible de voir le métavers non pas comme un lieu, mais plutôt comme une époque, dans le sens où le métavers allait marquer le basculement dans une nouvelle ère, celle où nos vies deviendraient plus numériques que physiques. Pour Mark Zuckerberg, ce moment charnière se produira lorsque la majorité des gens auront besoin du métavers pour leurs activités. **(2)** Afin de rester dans la course, Microsoft s'est offert pour 69 milliards de dollars l'éditeur de jeux vidéo Activision. Satya Nadella, président de la multinationale informatique américaine, se félicite de cette acquisition qui va lui permette de « posséder des composants essentiels pour le métavers » car « le jeu... jouera un rôle clé dans le développement des plateformes du métavers ». **(3)**

▪ Les géants de la technologie ne sont pas les seuls à vouloir s'implanter dans le métavers. D'autres acteurs, dont Decentraland et Sandbox, jouent des coudes et tentent d'imposer un autre type de métavers, reposant cette fois-ci sur un mode décentralisé. Dans ce « métavers crypto », la propriété du métavers est partagée entre ses utilisateurs au moyen de la technologie de la blockchain et des organisations autonomes décentralisées (DAO). De cette façon, les utilisateurs contrôlent l'avenir de ces métavers. Ces métavers aspirent à devenir des sociétés

REFERENCES

(1) Wikipedia, https://en.wikipedia.org/wiki/Metaverse#cite_note-O'Brian-Chan-1 Citant O'Brian, Matt; Chan, Kelvin (28 octobre 2021). "EXPLAINER: What is the metaverse and how will it work?". ABC News. Associated Press.

(2) Podcast « Mark in the Metaverse Facebook's CEO on why the social network is becoming a metaverse company » Newton, Casey, 22 juilllet, 2021. https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview.

(3) Microsoft's metaverse plans are getting clearer with its $68.7 billion Activision acquisition, Huddleston, Tom January 21, 2021 https://www.cnbc.com/2022/01/19/microsoft-activision-what-satya-nadella-has-said-about-the-metaverse.html

à part entière avec une économie propre et une organisation démocratique. A cette fin, ils ont recours aux NFT (jetons non fongibles), qui sont des objets numériques basés sur la blockchain. Chaque NFT est unique et permet d'authentifier la propriété de son contenu. Les NFT ont une valeur économique dans le monde réel et les jetons cryptos, objets et vêtements virtuels (« skin ») pour avatar, et biens immobiliers numériques peuvent tout à fait faire l'objet de transactions commerciales. (4)

(4) Cryptopedia, https://www.gemini.com/cryptopedia/what-is-metaverse-crypto-nft-game-blockchain

▪ Le métavers est en plein essor et une question essentielle se pose : qui, aux États-Unis, va réglementer ce nouveau monde ? Les autorités de régulation étatiques, les tribunaux ou les entreprises ? A dire vrai, il s'agira sera sans doute un peu des trois.

▪ De nombreuses lois fédérales américaines existantes sont naturellement susceptibles de s'appliquer au métavers : les lois sur la propriété intellectuelle, la fiscalité, les valeurs mobilières et le secteur bancaire, les jeux d'argent, la monnaie, la concurrence, les pratiques anticoncurrentielles et commerciales déloyales, la cybersécurité, l'emploi, le handicap, la protection des enfants... Toutefois, le problème est que ces lois sont inadaptées aux nouvelles problématiques soulevées par le métavers. C'est le cas, par exemple, pour ce qui concerne l'étendue du droit d'utilisation du contenu détenu par un propriétaire de NFT.

▪ De nouvelles lois sont par conséquent nécessaires, mais le législateur américain est pour le moment trop lent, préférant adopter une attitude attentiste. En outre, les Etats-Unis étant un état fédéral, la législation américaine s'en remet souvent aux lois des différents États fédérés, ce qui peut aboutir à un patchwork de lois différentes et parfois contradictoires d'un Etat à l'autre. C'est la raison pour laquelle, par exemple, qu'en l'absence d'un cadre législatif fédéral unique sur la protection des données personnelles, les lois de l'Etat de Californie en la matière se sont imposées comme une norme dans l'ensemble des États-Unis, alors même que ces lois ne sont normalement pas contraignantes en dehors du sol californien.

▪ Bien que le métavers n'en soit qu'à ses débuts, les premiers contentieux liés au métavers se multiplient déjà :

- Hermès « MetaBirkins » : la maison de luxe Hermès a assigné, devant le tribunal fédéral de New York, l'artiste M. R. en contrefaçon, ce dernier ayant créé une version NFT nommée « MetaBirkin », de son fameux sac Birkin (5) ;
- Recours collectif Kardashian/EMAX : des consommateurs ont intenté un procès en Californie à l'encontre de la star des réseaux sociaux Kim Kardashian, lui reprochant d'avoir fait la promotion de la cryptomonnaie EthereumMax, sans les mettre en garde contre le caractère volatil de ce produit d'investissement. Les plaignants affirment qu'il s'agit d'une arnaque reposant sur une technique de manipulation de marché (dite de « pump and dump ») qui consiste à inciter le plus grand nombre de personnes possible à investir dans une cryptomonnaie afin de faire gonfler sa valeur artificiellement, puis les escrocs revendent leurs actifs lorsque le cours de la monnaie atteint un pic, provoquant ainsi son effondrement et faisant perdre une grande partie de leur mise aux investisseurs (6) ;

(5) Hermes International v. Mason Rothschild, Case no. 1:2022cv00384 US District Court for the Southern District of New York. https://dockets.justia.com/docket/new-york/nysdce/1:2022cv00384/573363

(6) Huegerich v. Gentile et. al, et al, Case 2:22-cv-00163, U.S. District Court for the Central District of California https://dockets.justia.com/docket/california/cacdce/2:2022cv00163/840865

- Tarantino/Miramax : les studios de cinéma Miramax qui ont produit le film Pulp Fiction, ont poursuivi en justice pour violation de marque et de droit d'auteur son réalisateur, Quentin Tarantino, qui envisageait de vendre des NFT créés à partir du scénario de son long-métrage. L'action intentée en Californie repose sur la violation de leur contrat de 1993 qui réservait les droits de propriété aux deux parties mais ne mentionnait pas de droit d'utilisation à titre de NFT, alors inexistant **(7)** ;
- Jay-Z (Roc-A-Fella Records)/Damon Dash : Roc-A-Fella Records, le label de musique cofondé par le rappeur américain Jay-Z a réussi à obtenir d'un tribunal fédéral de New York l'interdiction de la vente de la version NFT d'un album de Jay-Z par Damon Dash, un autre cofondateur du label **(8)**, pour atteinte aux droits de propriété intellectuelle ;
- recours collectif en Californie contre Coinbase concernant une loterie: les participants à une loterie (*sweepstake*) organisée par la plateforme d'échange de cryptomonnaies Coinbase soutiennent que les 78 crypto-actifs concernés par cette loterie (dont le Dogecoin) seraient des « valeurs mobilières non autorisées ». A noter que cette action en justice opère une distinction entre les crypto-jetons et le Bitcoin et l'Ethereum en raison de la nature décentralisée de ces derniers. En jeu : le remboursement de l'intégralité de l'argent investi dans ce jeu concours **(9)** ;
- recours collectif en Californie contre Coinbase pour publicité mensongère : les plaignants, qui ont acheté des Dogecoins pour participer à un concours organisé par Coinbase, soutiennent que la plateforme aurait dû leur offrir, de manière claire, conformément à la loi californienne, la possibilité de participer gratuitement à ce concours, sans obligation d'achat .

(7) Miramax, LLC v. Tarantino Case 2:21-cv-08979-FMO-JC U.S. District Court for the Central District of California https://casetext.com/case/miramax-llc-v-tarantino

(8) Roc-A-Fella Records, Inc. v. Dash 1:2021cv05411, US District Court for the Southern District of New York, https://dockets.justia.com/docket/new-york/nysdce/1:2021cv05411/562168

(9) Suski v. Marden-Kane, Inc., 2022 WL 103541 (U.S. District Court Northern District of California)

▪ Il ne s'agit là que d'exemples parmi tant d'autres, au vu de l'avalanche de procès en cours ou à venir concernant le flot de questions inédites soulevées par ce monde virtuel émergent.

▪ Par ailleurs, l'application des lois étatiques et fédérales américaines se heurte au fait que le métavers soit un espace sans frontières. A cet égard, une décision récente de la Cour suprême des États-Unis pourrait faciliter l'autorégulation du métavers par les entreprises. Par une décision adoptée à 5 voix contre 4 dans l'affaire Netchoice v. Paxton 595 US (2022), la Cour suprême a suspendu l'entrée en vigueur d'une loi texane qui aurait interdit aux réseaux sociaux de bannir des utilisateurs en raison de leurs opinions, quand bien même leur propos seraient offensants ou erronés. La plus haute juridiction américaine a également refusé d'appliquer une clause de cette loi qui aurait obligé un réseau social à motiver les exclusions d'utilisateurs, restreignant ainsi leur liberté de modérer les contenus comme ils le souhaitent. Il convient cependant de nuancer la portée de cette décision qui n'est que temporaire et qui protège ainsi le statu quo jusqu'à ce que la Cour suprême publie sa décision finale sur la question de l'application du premier amendement aux réseaux sociaux.

▪ Dès lors, à moins que la Cour suprême des États-Unis ne finisse par les priver de leur autonomie de décision à l'égard de leurs utilisateurs, les réseaux sociaux disposent de la marge de manœuvre technologique nécessaire pour encadrer le

métavers et ses dérives. Par exemple, alors qu'elle testait la version bêta d'un produit Meta en réalité virtuelle, une femme a signalé que son avatar avait été harcelé verbalement et sexuellement : des avatars avaient formulé des remarques de nature sexuelle et « touché et tripoté » son avatar, tandis que d'autres la prenaient en photo pendant qu'elle subissait ces actes. Meta a réagi rapidement et créé, par défaut, une zone tampon de 60 centimètres autour de tous les avatars, empêchant ainsi les avatars de s'approcher de trop près. Cette zone tampon a ensuite été rapidement déployée sur l'ensemble des plateformes Meta, limitant de fait les interactions entre avatars aux salutations de type poing contre poing ou paume contre paume.

▪ Autre solution pour réguler le métavers : le recours aux « *smart contracts* ». Ces contrats intelligents sont en fait des codes numériques programmés qui s'exécutent sur la blockchain, automatisent les opérations et garantissent que les échanges et les transactions se font selon des règles prédéterminées. Ils peuvent servir à payer automatiquement des redevances, acheter et vendre des NFT, faire des dons et bien plus encore. Ils ont pour avantage d'être rapides et efficaces, sans nécessiter aucune paperasse. Les contrats intelligents sont également difficiles à falsifier ou à modifier. En revanche, leur nom est trompeur car il ne s'agit pas de contrats juridiquement contraignants, mais plutôt d'un ensemble de règles qui contrôlent l'utilisation de certains NFT. Les parties à ce type de contrat doivent être vigilantes car un contrat intelligent n'offre pas nécessairement les mêmes avantages aux acheteurs subséquents qu'au propriétaire initial.

▪ Enfin, les jetons cryptographiques sont une autre piste à explorer pour la régulation du métavers. En effet, ces jetons (tels que l'ERC-20), intégrés aux blockchains existantes, peuvent représenter non seulement des actifs tangibles (biens immobiliers, œuvres d'art etc.) mais également des actifs intangibles (droits de vote) et donc participer au mécanisme de gouvernance pour les entreprises. Sur les plateformes décentralisées, comme Sandbox, les jetons peuvent être utilisés dans le cadre du processus de prise de décision, ce qui permet d'avoir son mot à dire dans l'orientation stratégique future de la plateforme. Bien que la gouvernance décentralisée soit en constante évolution, les principaux processus sont en train d'être formalisés afin que les protocoles puissent être appliqués de manière équitable.

▪ Afin de de bénéficier d'une protection supplémentaire dans le cadre des lois américaines existantes en matière de propriété intellectuelle, certaines entreprises, dont Nike, déposent de multiples demandes de marques pour des biens virtuels. Toutefois, ces demandes sont fondées sur une intention d'usage (*intent to use*), de sorte que leur finalisation est conditionnée à une exploitation commerciale sur le territoire américain.

▪ Petit à petit, le métavers, se développe et va évoluer au-delà de nos rêves les plus fous, posant de nouvelles questions juridiques. Des solutions créatives et innovantes devront être trouvées si l'on veut permettre au métavers d'atteindre son plein potentiel.

JANICE F. MULLIGAN

usa@
lexing.network

Metaverse: What Regulation? U.S. Laws and Regulation by Speculation

▪ *The word "meta" is Greek for beyond. With historic roots in science fiction, meta was first defined in a 1992 book called Snow Crash by Neal Stephenson as a virtual universe controlled and owned by a "global information monopoly that users can access via personal VR goggles." Still now in its infancy, there is currently no truly such united place for "the" metaverse to be experienced. Numerous virtual worlds do exist and technology is beginning to bring together virtual content which never before existed and with it, it is creating legal challenges never before imagined.*

▪ *The goal is for the metaverse to embody the evolution of the Internet into "a single, universal and immersive virtual world that is facilitated by the use of virtual reality (VR) and augmented reality (AR) headsets." **(1)** Interfaces will also include body armor (haptic feedback suits) and nunchucks which will help one feel totally immersed in the experience.*

▪ *The metaverse promises to bring the virtual world to life! In a proprietary virtual 3D space, a person will take the form of an avatar and move freely to do much of what one does in the "real" world including shop, take classes, work, attend concerts, exercise, compete in sporting events, own assets and make creative and financial investments that can be sold.*

▪ *Metaverse is big business. Corporations seeks to maximize monetary transactions for the huge tech companies. For example, Facebook renamed its parent corporation "Meta" and committed US$180 billion dollars to develop the metaverse. Mark Zuckerberg said it is a "reasonable construct" for the metaverse to be a time, not a place. Some have pondered if the metaverse is a moment when our lives will become more digital than physical. Zuckerberg opined that this will likely happen once the masses need the metaverse to do their jobs. **(2)** Not to be locked out of the market, Microsoft acquired Activision for US$69 billion. According to Satya Nadella, chairman and CEO at Microsoft, the purchase of Activision "provide[s] building blocks for the metaverse and "gaming…will play a key role in the development of metaverse platforms." **(3)***

▪ *Corporate tech giants are not the only ones staking out turf in the metaverse. A different, decentralized crypto metaverse is also marching towards the future. Companies using this business model include Decentraland and Sandbox. Key features of such systems have the following characteristics: The ownership of the metaverse is shared by its users through the implementation of blockchain technology. Decentralized autonomous organizations (DAOs) put users in control of the game's future. These metaverses hope to grow into entire societies with economies and democratic leadership. Nonfungible tokens (NFTs) are digital objects on a blockchain. Because every NFT is unique, tokens are coded to prove*

REFERENCES

(1) Wikipedia, https://en.wikipedia.org/wiki/Metaverse#cite_note-O'Brian-Chan-1 Citing O'Brian, Matt; Chan, Kelvin (28 October 2021). "EXPLAINER: What is the metaverse and how will it work?". ABC News. Associated Press.

(2) Podcast Mark in the Metaverse Facebook's CEO on why the social network is becoming a metaverse company" Newton, Casey July 22, 2021. https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview.

(3) Microsoft's metaverse plans are getting clearer with its $68.7 billion Activision acquisition, Huddleston, Tom January 21, 2021 https://www.cnbc.com/2022/01/19/microsoft-activision-what-satya-nadella-has-said-about-the-metaverse.html

(4) Cryptopedia, https://www.gemini.com/cryptopedia/what-is-metaverse-crypto-nft-game-blockchain

ownership of user-generated content and NFT assets. These tokens have real-world economic value. Holders of crypto tokens, avatar skins, and digital real estate can trade them. ***(4)***

▪ *With the power grab for this burgeoning new field accelerating, a critical question is who will regulate this unsettled field in the United States? Will it be government regulators, courts, or corporate self-governance rising to the occasion? It will likely be a combination of all three.*

▪ *Existing U.S. federal laws likely to play a role include intellectual property, tax, securities/banking, gambling/lottery, currency, antitrust, unfair trade practices, cybersecurity, employment, disabilities act and statutes for the protection of children. One of the problems with these existing laws is that they are inadequate for novel issues raised by the metaverse, (such as the scope of the right to use content held by an NFT owner.)*

▪ *New laws are needed, but U.S. regulators are too slow, preferring to take a "wait and see" attitude. Additionally, U.S. law often defers to individual state laws, which are fractured and inconsistent. For example, with no existing body of federal privacy laws, California's privacy statutes have become the gold standard in the United States, even though such laws are not binding outside this state.*

▪ *While the metaverse industry may be in its infancy, there is already a growing body of litigation, including:*

- *Hermès "MetaBirkins": Claiming misappropriation of intellectual property rights, a cease and desist order was filed in the U. S. Dist. Ct. NYC against an artist who made a NFT version of the Hermes Birkin bag.* ***(5)***

- *Kardashian/EMAX Class Action: Consumers sued in California under the state's consumer protection laws. The suit arose from Kim Kardashian's social media endorsement which failed to disclose that an NFT is a volatile investment product. The suit claims this was a classic "pump and dump" causing the NFT's value to plummet.* ***(6)***

- *Tarantino/Miramax: Tarantino minted NFTs from the Pulp Fiction screenplay. The film studio sued in California for breach of trademark and copyright arising from a 1993 contract that reserved both parties' property rights but was silent on the then nonexistent right to use such property for NFTs.* ***(7)***

- *Jay-Z (Roc-A-Fella Records)/Damon Dash: A violation of intellectual property rights was adjudicated in the federal court in NYC against the record company's co-founder Dash, enjoining him from auctioning a NFT of Jay-Z's album cover.* ***(8)***

- *Coinbase/Dogecoin Sweepstakes California Class Action: Claiming Dogecoin and 78 other crypto tokens are allegedly "unlicensed securities", this lawsuit distinguishes crypto tokens from Bitcoin and Ethereum*

(5) Hermes International v. Mason Rothschild, Case no. 1:2022cv00384 US District Court for the Southern District of New York. https://dockets.justia.com/docket/new-york/nysdce/1:2022cv00384/573363

(6) Huegerich v. Gentile et. al, et al, Case 2:22-cv-00163, U.S. District Court for the Central District of California https://dockets.justia.com/docket/california/cacdce/2:2022cv00163/840865

(7) Miramax, LLC v. Tarantino Case 2:21-cv-08979-FMO-JC U.S. District Court for the Central District of California https://casetext.com/case/miramax-llc-v-tarantino

(8) Roc-A-Fella Records, Inc. v. Dash 1:2021cv05411, US District Court for the Southern District of New York, https://dockets.justia.com/docket/new-york/nysdce/1:2021cv05411/562168

because of the latter's decentralized nature. The return of all investors' money is claimed as damages. ***(9)***

- *Coinbase/Dogecoin False Advertising California Class Action: Sweepstakes rules must offer a free form of entry. Class representative claims he wouldn't have paid to enter the contest if Coinbase had clearly disclosed there was a free way to enter the contest.*

(9) Suski v. Marden-Kane, Inc., 2022 WL 103541 (U.S. District Court Northern District of California

▪ *The above are only examples of the multitude of lawsuits filed over various novel issues raised in this emerging virtual world.*

▪ *Enforcement of any such state and federal laws are hampered by the lack of borders in the Metaverse. A new U.S. Supreme Court decision may make it easier for corporate selfgovernance, at least for now. With a 5-4 split decision in* Netchoice v. Paxton 595 US __ (2022)*, the Court stayed a Texas law from going into effect which would have prohibited social media companies from banning users over their viewpoints, even if their rhetoric is offensive or erroneous. The Court also refused to enforce a statutory clause which would have required corporations to explain and disclose reasons for any individual to be banned from the website. Unfortunately, this is only a temporary ruling protecting the status quo until the Court publishes its final ruling on the issue of how the first amendment applies to social media.*

▪ *Absent the U.S. Supreme Court stripping corporations from self-governance over participants' speech, these companies are in a superior position to use technology to police the metaverse. For example, while beta-testing a Meta product in virtual reality, a female reported her avatar was verbally and sexually harassed with sexual innuendos and other avatars "touched and groped" her avatar while yet other avatars took selfie photos. With a quick response to this problem, Meta used technology to create a two-foot personal boundary around all avatars by default, thus blocking wayward hands from drawing too close. The forcefield style safety mechanism was then quickly rolled out across all Meta platforms, limiting interactions between avatars to fist bumps and high fives.*

▪ *Another technological solution to help to regulate the metaverse is the use of "smart contracts". These are programmed digital codes that run on the blockchain, automate operations, and ensure that trading and transactions are done according to predetermined rules. They can be programmed to automatically pay royalties, buy and sell NFTs, make donations and much more. Benefits include speed and efficiency, without any paperwork to process. Smart contracts are also hard to hack or alter. On the downside, their name is misleading because they are not actually legally binding contracts, but rather a set of rules that control the use of specific NFTs. Subsequent purchasers may also be mislead because a smart contract does not necessarily provide the same benefits to all downstream purchasers as it does for the original owner.*

▪ *Crypto tokens are also novel mechanism for corporate governance. Crypto tokens (such as ERC-20) are built into existing blockchains. Some crypto tokens represent*

tangible assets such as real estate or art, while others represent intangible assets, including governance voting rights on the platform. In decentralized platforms such as Sandbox, crypto tokens can be used as a method of decision making to guide the future direction of various blockchain projects. While decentralized governance is still evolving, key processes are being standardized and implemented so that protocols can be equitably enforced.

▪ *Striving to obtain "extra" protection under existing intellectual property laws, some companies, including Nike, are filing multiple applications seeking U.S. trademark protection for virtual goods. Such applications are on an intent-to-use-basis, so they won't be finalized in the U.S. until they are in commercial use.*

▪ *As we dive deeper into the metaverse, it will expand and evolve beyond our wildest dreams, and with it, novel legal and regulatory issues will arise. Creative and innovative solutions must be found if the metaverse is to meet its full potential.*

JANICE F. MULLIGAN

usa@
lexing.network

IA : la réglementation européenne prend forme

▪ La Commission a rendu public au printemps dernier son projet de règlement sur l'intelligence artificielle qui, lorsqu'il sera définitivement adopté, constituera la clé de voûte de la future réglementation européenne en la matière.

Le projet de règlement européen sur l'IA

▪ La Commission européenne a présenté le 21 avril 2021 une proposition de règlement sur l'intelligence artificielle **(1)**. Celle-ci fait suite à l'important travail mené par le Parlement européen dans ce domaine, qui avait déjà donné lieu en octobre 2020 à l'adoption d'un certain nombre de résolutions et projets de directives relatives à l'IA **(2)** concernant les aspects éthiques, le régime de responsabilité et les droits de propriété intellectuelle.

▪ Le nouveau règlement vise à de promouvoir une IA *« digne de confiance »* tout en tenant compte des risques associés à certaines de ses utilisations, notamment au plan des libertés individuelles et de la sécurité des utilisateurs.

▪ Pour ce faire, la Commission a choisi d'adopter une démarche fondée sur l'analyse des risques que les systèmes d'IA présentent, avec en filigrane l'éthique et la dignité.

Une approche fondée sur l'analyse des risques

▪ Cette approche l'amène à distinguer trois groupes de systèmes d'IA :

- Les systèmes « interdits » car jugés incompatibles avec les valeurs fondamentales communes aux pays de l'UE, tels que le respect de la dignité humaine et des droits de l'homme. Ces valeurs se traduisent par l'interdiction de certaines pratiques d'IA telle que la manipulation des personnes vulnérables ou l'identification biométrique en temps réel dans l'espace public aux fins de police (sauf dans certaines situations précisément répertoriées et définies) **(3)** ;
- Les systèmes présentant un risque limité, faible ou minimal et qui ne sont soumis qu'à des obligations de transparence d'information sur la présence de l'IA (chatbots, dialogueurs ou systèmes de trucage vidéo ultra réalistes de jeux vidéo, filtres antispam…) ;
- Les systèmes dits « à haut risque ».

Les systèmes d'IA à « haut risque »

▪ Les systèmes d'intelligence artificielle à risque élevé sont de deux types :

- ceux couverts par une des législations européennes figurant sur la liste de l'annexe 2 du projet de Règlement (systèmes d'IA concernant l'aviation civile, certains véhicules type quadricycles ou encore les dispositifs médicaux) ;

REFERENCES

(1) Règlement du Parlement européen et du Conseil établissant des règles harmonisées concernant l'intelligence artificielle, COM (2021) 2016

(2) Cf. A. Bensoussan, Les lois de l'IA à l'horizon 2021, Planète robots n°66 février-mars 2021, p.10

(3) Par exemple, pour rechercher les victimes d'infraction (enfants disparus), lutter contre certains types d'infractions ou prévenir une attaque terroriste

- ceux figurant sur la liste de l'annexe 3 du projet de Règlement (infrastructures critiques (énergie et transports), éducation, emploi…).

▪ Ils sont soumis à un certain nombre d'obligations : analyse et gestion des risques, évaluation et déclaration de conformité, transparence, garanties en matière de sécurité ou de correction face aux risques de biais, d'erreurs et d'opacité.

▪ Les systèmes d'identification biométrique à distance fondés sur l'IA, sont considérés à haut risque et la Commission rappelle l'interdiction de leur utilisation dans l'espace public et en temps réel *« aux fins du maintien de l'ordre »* en dehors de cas spécifiques encadrés judiciairement.

Garantir aux Européens qu'ils peuvent faire confiance à l'IA

▪ La Cnil et ses homologues européens ont remis un avis dans lequel ils préconisent de ne focaliser l'effort de régulation que sur les systèmes d'IA dit « à haut risque » pour les droits fondamentaux **(4)**.

▪ De son côté, le Haut-Commissariat de l'ONU aux droits de l'homme (HCDH) appelle à imposer un moratoire sur certains systèmes d'IA comme la reconnaissance faciale, le temps de *« mettre en place un dispositif pour protéger les droits humains quant à leur utilisation »* **(5)**.

▪ Ce texte doit désormais être examiné par le Parlement européen au cours des prochains mois dans le cadre de la procédure législative ordinaire. Une fois adoptées, ces nouvelles règles seront directement applicables dans tous les États membres à tout système d'IA ou à tout produit en contenant.

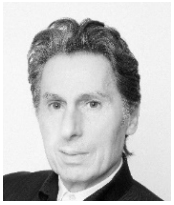
▪ *« Proportionnées et souples pour faire face aux risques spécifiques liés aux systèmes d'IA, celles-ci constitueront, selon la Commission, l'ensemble de normes le plus strict au monde »* **(6)**. Qu'on en juge : les amendes encourues par les entreprises pourront atteindre 30 millions d'euros ou 6% du chiffre d'affaires annuel mondial total, notamment en cas non-conformité du système d'IA avec les exigences du règlement **(7)**.

(4) Avis conjoint 5/2021 du 18-06-2021 sur la proposition de règlement IA (en anglais), CEPD

(5) ONU Info, Communiqué du 15 septembre 2021

(6) De nouvelles règles et actions en faveur de l'excellence et de la confiance dans l'intelligence artificielle, Commission européenne, communiqué du 21 avril 2021

(7) Art. 71 de la proposition de règlement



ALAIN BENSOUSSAN

france
@lexing.network

REFERENCES

AI: European regulation is taking shape

▪ *Last spring, the European Commission published its draft regulation on artificial intelligence which, when finally adopted, will be the cornerstone of future European regulation in this area.*

The draft European AI regulation

▪ *On 21 April 2021, the European Commission presented a proposal for a regulation on artificial intelligence* ***(1)****. This follows the considerable amount of work undertaken by the European Parliament in the area of AI, which had already led to the adoption in October 2020 of a number of resolutions and draft directives related to AI* ***(2)*** *including on ethics, liability and intellectual property rights.*

▪ *The new regulation aims to promote "*trustworthy*" AI while addressing the risks associated with certain of its uses, in particular in terms of individual freedoms and user safety.*

▪ *To this end, the Commission has chosen to adopt an approach based on an analysis of the risks that AI systems present, especially with regard to ethics and human dignity.*

A risk-based approach

▪ *This* risk-based *approach leads it to distinguish three groups of AI systems:*

- *"Prohibited" systems, as they are deemed incompatible with fundamental values common to EU countries, such as the respect for human dignity and human rights. These values are reflected in the prohibition of certain AI practices such as the manipulation of vulnerable persons or real-time biometric identification in publicly accessible spaces for law enforcement purposes (except in exhaustively listed and narrowly defined situations)* ***(3)****;*
- *Systems presenting a limited, low or minimal risk and which are only subject to transparency obligations which require that people be informed of the presence of AI (such as chatbots, deep fakes, spam filters);*
- *So-called "high-risk" systems.*

"High risk" AI systems

▪ *High risk AI systems are of two types:*

- *those covered by any of the European legislation listed in Annex II of the draft Regulation (e.g. AI systems concerning civil aviation, certain quadricycles or medical devices);*
- *those listed in Annex III of the draft Regulation (e.g. critical infrastructure (energy and transport), education, employment).*

(1) Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence, COM (2021) 2016

(2) A. Bensoussan, Les lois de l'IA à l'horizon 2021, Planète robots n°66 février-mars 2021, p.10

(3) For example, to search for victims of crime (including missing children), to combat certain types of crime or to prevent a terrorist attack

▪ *They are subject to a number of obligations: risk analysis and management, assessment and declaration of conformity, transparency, security guarantees or correction in relation to the risks of potential biases, errors and opacity.*

▪ *AI-based remote biometric identification systems are classified as high risk and the EU Commission recalls the prohibition of their use in in publicly accessible areas and in real time "for the purpose of law enforcement" except in specific cases subject to judicial oversight.*

Ensuring that Europeans should be able to trust AI

▪ *The CNIL and its European counterparts have submitted an opinion in which they recommend focusing regulatory efforts only on "high risk" AI systems for fundamental rights* ***(4)****.*

▪ *The Office of the UN High Commissioner for Human Rights (OHCHR) called for a moratorium on certain AI systems, such as facial recognition, while a mechanism is put in place to protect human rights* ***(5)****.*

▪ *The draft Regulation is now due to be reviewed by the European Parliament in the coming months under the ordinary legislative procedure. Once adopted, the new rules will be directly applicable in all Member States to any AI system or product containing AI.*

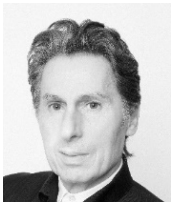
▪ *"Proportionate and flexible to address the specific risks associated with AI systems, they will be, according to the Commission, the strictest set of standards in the world"* ***(6)****. 30 million or 6% of the total annual worldwide turnover, in particular in case of non-compliance of the AI system with the requirements of the regulation* ***(7)****.*

(4) EDPB-EDPS Joint Opinion 5/2021 of 18-06-2021 on the proposal for an Artificial Intelligence Act

(5) UN News, press release of 15 September 2021

(6) De nouvelles règles et actions en faveur de l'excellence et de la confiance dans l'intelligence artificielle, Commission européenne, communiqué du 21 avril 2021

(7) Art. 71 de la proposition de règlement



ALAIN BENSOUSSAN

france
@lexing.network

Le secteur des jeux dans le métavers

Le présent article résume l'intervention de Lexing Grèce lors la conférence mondiale Lexing sur le thème du secteur des jeux dans le métavers. Cette présentation vise à identifier les caractéristiques principales du métavers, les possibilités de développement d'activités liées au secteur des jeux dans les métavers, et les enjeux juridiques associés.

▪ L'industrie des jeux d'argent en ligne, déjà florissante, est en passe de connaitre un nouvel essor grâce aux nouvelles possibilités offertes par le métavers. Reste à savoir jusqu'à quel point.

▪ Le métavers présente trois caractéristiques principales :

- il s'agit d'une technologie qui permet au contenu numérique de se superposer au monde réel ;
- il permet, grâce à un équipement approprié, d'interagir avec le monde réel, avec des fonctionnalités de réalité augmentée ou de réalité virtuelle ;
- il contient des informations sur tout ce qui se trouve dans le monde physique (par exemple, un lieu, un magasin ou un produit) ainsi que sur l'utilisateur (son emploi du temps, sa localisation, ses habitudes et ses intérêts etc.) **(1)**.

▪ Le métavers va ainsi constituer un univers virtuel qui améliorera d'innombrables aspects de la réalité physique, offrant des possibilités illimitées d'activités dans tous les domaines, que ce soit des services financiers, des plateformes sociales et même des événements en direct. Le secteur des jeux, ou ce que l'on nomme plus généralement le « divertissement compétitif », ne fait pas exception. Paris sportifs, fantasy sports, e-sports, jeux vidéo, courses de chevaux, casinos virtuels, et bien d'autres encore, vont très certainement investir le métavers.

▪ Les casinos dans le métavers peuvent ainsi servir d'extensions aux casinos en ligne ou aux plateformes de paris traditionnelles, à ceci près que toutes les transactions seront réalisées en crypto-actifs. La technologie blockchain garantit un niveau élevé de transparence, de sécurité et de confidentialité aux jeux de hasard en cryptomonnaies. Autre avantage : les gains et les paris sont enregistrés sur la blockchain et, bien souvent, un « crypto casino » ne facturera pas de frais lors de la participation à un tournoi de poker ou à d'autres événements de jeu. Les joueurs apprécieront également le fait que leurs paris ne puissent pas être truqués en faveur de la maison. **(2)**.

▪ Des risques existent naturellement. Tout d'abord, les jeux d'argent pratiqués par des voies illégales ou non réglementées, que ce soit à l'arrière d'un bar, sur des machines non réglementées ou dans le métavers, peuvent présenter des risques pour les consommateurs **(3)**. Ce type d'activités, souvent liées au blanchiment d'argent ou à d'autres activités criminelles, ne permettent ni aux consommateurs

(1) Reed Smith, Guide to the Metaverse, Issue 1 - Mai 2021

(2) Rachel Breia, Metaverse Casinos: Gambling In Virtual Worlds, last accessed on July 18, 2022 at https://sensoriumxr.com/articles/metaverse-casinos-gambling-in-virtual-worlds

(3) Rob Lenihan, The Metaverse Has a Winner: Casinos, Gamblers, last accessed on July 18, 2022 at https://www.thestreet.com/investing/cryptocurrency/the-metaverse-has-a-winner-casinos-gamblers

de bénéficier de la protection qui leur est dû, ni aux Etats d'engranger les taxes associées.

▪ Autre difficulté : la détermination du droit national applicable au métavers. A cet égard, plusieurs éléments sont susceptibles de jouer un rôle. L'expérience acquise par les législateurs européens au cours des dernières décennies conduira très probablement à des solutions déjà éprouvées, comme l'application de loi de l'État membre de l'entité concernée dans l'Union européenne.

▪ En outre, les casinos dans le métavers fonctionneront probablement avec des crypto-actifs. Or, pour l'instant, les crypto-actifs ne sont pas considérés par la législation de l'UE comme des instruments financiers ou de la monnaie électronique, et la proposition de règlement européen sur les marchés de crypto-actifs (dit règlement MiCA) **(4)**, ne rentrera pas en vigueur avant 2024. D'où l'existence d'une incertitude juridique entourant les transactions de ces crypto-actifs. Le cadre juridique de la lutte contre le blanchiment d'argent et le financement du terrorisme dans les pays de l'UE **(5)** prévoit déjà, quant à lui, l'obligation pour les États membres de surveiller les prestataires de services de portefeuilles de conservation et de services d'échange entre monnaies virtuelles et monnaies légales.

▪ Enfin, il va de soi que les criminels sont attirés par les espaces peu réglementés où les flux d'argent sont importants. Tandis que les forces de l'ordre s'attèlent d'ores et déjà à déployer des techniques de surveillance dans le métavers, il n'est pas encore clair sous quelle forme la criminalité traditionnelle va se traduire dans le métavers. Si la fraude ou l'extorsion sont facilement transposables dans l'environnement numérique du métavers, ce n'est en effet pas le cas des actes de violence par exemple. A ce jour, on peut se demander si les infractions ayant lieu dans le métavers seront punies par les tribunaux publics, sur le fondement de la violation des dispositions pénales, ou par les tribunaux privés dans le métavers, sur le fondement de la violation des conditions générales d'utilisation. **(6)**.

▪ Avec les progrès spectaculaires de la technologie, des équipements et des réseaux de communication, le métavers est porteur à la fois de possibilités nouvelles et de complications juridiques. C'est dans ce paysage juridique passionnant que les acteurs du monde juridique seront appelés à mettre en œuvre les réglementations existantes en matière de jeux d'argent ou à en élaborer de nouvelles, adaptées aux nouvelles conditions et aux nouveaux besoins. **(7)**

(4) Proposition de Règlement du Parlement Européen et du Conseil sur les marchés de crypto-actifs, et modifiant la directive (UE) 2019/1937

(5) Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n°648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, ainsi que la législation nationale de transposition

(6) Garon, Jon M., Legal Implications of a Ubiquitous Metaverse and a Web3 Future (January 3, 2022). Available at SSRN: https://ssrn.com/abstract=4002551

(7) Murr
ay, Michael D., Ready Lawyer One: Lawyering in the Metaverse (April 12, 2022). Available at SSRN: https://ssrn.com/abstract=4082648

NIKOLAOS PAPADOPOULOS

greece@lexing.network

REFERENCES

Competitive entertainment in the metaverse

This is a high-level analysis of Lexing Greece presentation in Lexing World Conference on competitive entertainment in the metaverse. Our presentation aimed to identify the basic elements of metaverse, how these elements enable the development of gambling and betting entities in the metaverse, and finally potential legal issues and controversies.

▪ *Online gambling is a huge industry, which is poised to become even larger by deploying novel possibilities for users and customers in the metaverse. The nature, the elements, and the exact problems of the convergence of the online competitive entertainment and the metaverse can only be speculated for now.*

▪ *We identify three main elements of the metaverse:*

- *it is a technology that enables the digital content to be laid over the real world;*
- *it includes a hardware device that enables the real world to be interactive, with Augmented Reality or Virtual Reality features;*
- *it contains information about anything and everything in the physical world (for instance, an area, a shop, or a product) and knowledge about the user (such as the user's schedule, location, habits, and interests)* ***(1)****.*

▪ *The Metaverse will become a virtual universe enhancing countless aspects of physical reality, hosting endless applications and limitless possibilities, including games, financial services, social platforms, and even depictions of live events. A Metaverse casino reunites all these aspects into an interactive product for virtual users. In this atmosphere of extraordinary user-engagement, companies that fit within the umbrella of "Competitive Entertainment" will be especially contributive to the fruition of the Metaverse. A wide array of businesses and industries, including Sports Betting, Fantasy Sports, Esports, Video Gaming, Horse Racing, Virtual Casinos, and more, will most certainly be interested in the possibilities of the metaverse.*

▪ *In this regard, metaverse casinos may serve as extensions of regular online casinos or betting platforms, where all transactions will be processed in crypto assets. This way, by relying on blockchain technology, crypto gambling ensures a higher level of transparency, security, and privacy. Winnings and bets are recorded on the blockchain and quite often a crypto casino won't charge fees when entering a poker tournament or other gambling events. Players may also welcome the idea that their bets are not being rigged in favour of the house* ***(2)****.*

▪ *It is evident that gambling occurring through illegal or unregulated channels, either in the back of a bar, through unregulated machines, or in the metaverse, may present risks to consumers* ***(3)****. Such unregulated gambling and betting operations remain beyond the spectrum of consumer protection, often tied to*

(1) Reed Smith, *Guide to the Metaverse*, Issue 1 - May 2021

(2) Rachel Breia, *Metaverse Casinos: Gambling In Virtual Worlds*, last accessed on July 18, 2022 at https://sensoriumxr.com/articles/metaverse-casinos-gambling-in-virtual-worlds

(3) Rob Lenihan, *The Metaverse Has a Winner: Casinos, Gamblers*, last accessed on July 18, 2022 at https://www.thestreet.com/investing/cryptocurrency/the-metaverse-has-a-winner-casinos-gamblers

money laundering or other criminal activities, and remains unclear how they will be taxed by each state.

- *The lack of obvious application of legal provisions, the difficulty in establishing national jurisdiction, a notion that law does not or will not apply in the metaverse are all factors taken into consideration in this comparison. The experience legislators accumulated during the last decades will most likely lead to previously tested solutions, such as assigning jurisdiction to the member state of the establishment in the EU.*

- *Metaverse casinos will probably operate with crypto assets. For the time being, crypto assets are not categorized by EU legislation as financial instruments or e-money and MiCA, EU's Proposal for a Regulation on Markets in Crypto-Assets* ***(4)****, will not be in force before 2024, thus creating legal uncertainty with regard to crypto transactions. Besides, the AML/CFT legal framework in EU countries* ***(5)*** *already sets out obligations for member-states to supervise entities providing custody services of digital wallets and exchange services between virtual currencies and fiat currencies.*

- *Moreover, criminal activities might be drawn towards sub-regulated spaces with excessive money flows. To be exact, off-metaverse law enforcement is already planning ways to deploy surveillance techniques in the metaverse. However, it is not clear yet how typical crimes will be translated in the metaverse. For example, the nature of crimes such as fraud or extortion allows for their straightforward interpretation in the digital environment of the metaverse, but this is not the case with crimes of violence. It remains unclear whether transgressions taking place in the metaverse will be punished by public courts, on the basis of criminal provisions or by private metaverse courts, on the basis of T&Cs infringement* ***(6)****.*

- *Driven by the dramatic evolutionary combination of technology, devices, and communication networks, the metaverse offers opportunities in the same ratio as it produces legal complications. This is the exciting scenery where we will be called upon to implement existing gambling regulations or draft new ones, tailored to new conditions and novel needs* ***(7)****.*

(4) Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937

(5) Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, as well as the national transposition legislation

(6) Garon, Jon M., *Legal Implications of a Ubiquitous Metaverse and a Web3 Future* (January 3, 2022). Available at SSRN: https://ssrn.com/abstract=4002551

(7) Murray, *Michael D., Ready Lawyer One: Lawyering in the Metaverse* (April 12, 2022). Available at SSRN: https://ssrn.com/abstract=4082648

NIKOLAOS PAPADOPOULOS
greece@lexing.network

La protection des données au Japon

1. Aperçu de la loi sur la protection des données personnelles (APPI) au Japon

▪ L'APPI s'applique à toute entité commerciale qui gère ou traite des données personnelles.

▪ Avant 2017, l'APPI ne s'appliquait pas aux entreprises qui traitaient moins de 5000 données personnelles, mais ce seuil quantitatif limitation a été supprimé en 2017.

▪ L'APPI s'applique en partie aux responsables du traitement étrangers qui, dans le cadre de la fourniture de biens ou de services à une personne au Japon, ont directement acquis des données personnelles relatives à cette personne.

▪ Les données personnelles sont définies comme toute information à partir de laquelle il est possible de déduire l'identité d'une personne vivante. Sont notamment inclus dans cette définition les marqueurs biométriques, les numéros d'identification officiels, etc.

▪ La définition ci-dessus s'applique indépendamment de la nationalité et du lieu de résidence de la personne.

2. Quels sont les conditions à respecter pour le transfert de données personnelles en dehors du Japon ?

▪ Au Japon, l'APPI a récemment été révisée au regard du RGPD, et désormais, certaines dispositions de l'APPI sont davantage alignées avec les dispositions du RGPD.

▪ Le principe général est qu'un responsable du traitement **(1)** doit obtenir le consentement préalable des personnes auxquelles se rapportent les données avant de les transférer à l'étranger.

(1) c'est-à-dire un opérateur commercial utilisant une base de données personnelles pour son activité

▪ Toutefois, des exceptions à ce principe existe. Par exemple, les transferts vers un pays étranger sont autorisés si ce pays étranger a été reconnu par le gouvernement japonais comme offrant des normes de protection des données personnelles équivalentes à celles garanties au Japon.

▪ L'existence de normes équivalentes s'apprécie selon les 5 conditions suivantes :

- le pays dispose d'une loi équivalente à l'APPI ;
- le pays dispose d'une commission indépendante en charge de la protection des données personnelles, équivalente à la commission japonaise ;
- le pays accepte de coopérer avec le Japon pour assurer la protection des données personnelles ;

- il est possible de transférer des données personnelles entre le pays et le Japon d'une manière qui garantit la protection desdites données ;
- l'autorisation de transfert accordée est bénéfique pour l'économie et les citoyens japonais.

▪ A ce jour, seuls l'Union européenne et le Royaume-Uni ont été officiellement reconnus par le gouvernement japonais comme satisfaisant aux exigences susmentionnées.

▪ Autre exception au principe général concernant les transferts transfrontaliers : des données personnelles peuvent être transférées vers un tiers situé dans un pays étranger si ce tiers respectent aux normes prescrites par le gouvernement japonais. Par exemple :

- le responsable du traitement et le tiers ont conclu un accord qui définit les moyens d'établir et de garantir ces normes ;
- le tiers dispose, entre autres, de règlements et de politiques internes permettant de garantir ces normes ;
- le tiers a été officiellement certifié par l'outil de transfert *Cross Border Privacy Rules (CBPR)* mis en place par l'APEC.

▪ Toutefois, pour que cette exception s'applique, le responsable du traitement doit, outre les mesures nécessaires pour garantir les normes, être en mesure de fournir, sur demande des personnes concernées, des informations sur le tiers destinataire situé dans le pays étranger **(2)** et notamment en :

(2) Cette disposition a été modifiée en 2022

- confirmant régulièrement le fonctionnement du tiers et les règles du pays étranger qui influent sur ce fonctionnement ;
- prenant des mesures appropriées et raisonnables et en suspendant les transferts en cas d'identification de situations pouvant mettre en cause le maintien des normes.

3. Comparaison entre l'APPI et le RGPD

▪ Il existe 5 différences notables entre l'APPI et le RGPD :

- (1) Il n'existe pas de droit à la portabilité des données dans l'APPI ;
- (2) Il n'existe pas de droit au retrait du consentement dans l'APPI (la suppression ou la rectification de données personnelles sont soumises à certaines conditions) ;
- (3) Concernant les catégories particulières de données personnelles :
  - l'APPI ne désigne pas clairement l'appartenance syndicale, la vie sexuelle ou l'orientation sexuelle d'une personne physique comme constituant des catégories particulières de données personnelles ;
  - cependant, des directives supplémentaires ont été établies par le gouvernement japonais pour que le responsable du traitement protège ce type de données.

- (4) Concernant la communication de données personnelles à un tiers, l'APPI prévoit des exceptions à l'obligation de consentement général plus larges que le RGPD :
    - dans l'APPI, si une notification préalable est donnée à la personne concernée et qu'un rapport est fait à la Commission de protection des données personnelles, aucun consentement n'est requis pour le transfert de données à un tiers.
- (5) Le montant maximal de l'amende sanctionnant une violation de l'APPI est nettement inférieur à celui prévu par le RGPD :
    - APPI : 100M yens, soit environ 713 000 euros ;
    - RGPD : 20 000 000 euros ou 4 % du chiffre d'affaires total, le montant le plus élevé étant retenu.

KOKI TADA

japan@
lexing.network

Data Protection in Japan Some Key Features

1. Overview of the Act on the Protection of Personal Information (APPI) in Japan

- *The APPI applies to any business entity that handles or processes personal information.*
- *Prior to 2017, the APPI did not apply to companies who handled less than 5000 items of personal information, but this limitation on the application of the APPI was deleted in 2017.*
- *The APPI partly applies to a personal information controller in a foreign company who has (in relation to supplying good or services to a person in Japan) directly acquired personal information relating to the person.*
- *Personal information is defined as any information from which one can deduce the identity of a living individual. Such information includes biometric markers, official identifier numbers, etc.*
- *The above definition applies regardless of the nationality and location of the person.*

2. What are the main principles when transfers of Personal Data in Japan are made to outside of Japan?

- *The APPI was revised with reference to the GDPR recently (i.e., some parts of the APPI are now more in line with the GDPR).*
- *As a general rule, it is necessary for a personal information controller* ***(1)*** *to obtain prior consent from the individuals who provide personal information before transferring it.*
- *However, as one of exceptions to the above-noted general rule, transfers to a foreign country are acceptable if the foreign country has been approved by the Japanese government as having equivalent standards (to Japan) for a personal information protection system.*
- *There are 5 requirements for determining the existence of equivalent standards:*
  - *there is an Act which is equivalent to the APPI in the country;*
  - *there is an independent personal information protection commission in the country which is equivalent to the commission in Japan;*
  - *the country has agreed to cooperate with Japan to protect personal information;*
  - *it is possible to transfer personal information between the country and Japan in a way that protects the personal information;*

(1) Business operator using a personal information database for its business

- *the approval is confirmed to be beneficial for new industry and the lives of citizens in Japan.*

▪ *The Japanese government has officially approved only the EU and UK as having satisfied these requirements as of today (no other countries have been approved yet).*

▪ *Also, as the other exception to the above-noted general rule, transfers may be made to a third party in a foreign country if such third party has a system which conforms to the standards prescribed by the rules of the Japanese government. For example:*

- *the personal information controller and the third party have entered into an agreement on ways to make and maintain the subject standards;*
- *the third party has internal regulations and policies, etc. to maintain the standards;*
- *the third party has been officially certified by "the Cross Border Privacy Rules" of APEC.*

▪ *For this exception to apply, the personal information controller needs to take the necessary action (such as the items noted below) for maintaining the standards and provide information on the third party in a foreign country when a person requests it* ***(2)****:*

(2) Amended in 2022

- *regularly confirm the operation of the third party and the rules of the foreign country which influence the operation;*
- *take appropriate and reasonable action and suspends transfers when recognizing anything that may interfere with the maintenance of the standards.*

3. Comparison between APPI and GDPR

▪ *There are 5 key differences between APPI and GDPR:*

- *(1) No Data Portability Right in the APPI.*
- *(2) No right of withdrawal of consent in the APPI (in order to delete or revise personal information, certain conditions must be met).*
- *(3) Special categories of personal information:*
  - *The APPI does not clearly describe "trade union membership, a natural person's sex life or sexual orientation" as special categories of personal information.*
  - *However, additional guidelines have been made by the Japanese government to have the personal information controller protect this type of information.*
- *(4) The APPI has wider exceptions to the general consent requirement when providing personal information to a third party.*

- *In the APPI, if prior notice is given to the individual and a report is made to the Personal Information Protection Commission, no consent is required for a transfer to a third party:*

- *(5) Maximum amount of penalty under the APPI is significantly lower than the GDPR:*
  - *APPI - Max: JPY100M ≒ EUR713,000*
  - *GDPR - Higher of EUR20,000,000 or 4% of total sales.*

KOKI TADA

japan@
lexing.network

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne *Germany*	Mercatorius	Guido Imfeld	+49(0)241 / 946 21-0	germany@lexing.network
Australie *Australia*	Gadens	Dudley Kneller	+61 438 363 443	australia@lexing.network
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Brésil *Brazil*	Andrea Filomeno Faria	Andrea Filomeno Faria	+55 11 2189 0061	brazil@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Cynthia Chassigneux	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Côte d'Ivoire *Ivory Coast*	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
États-Unis *USA*	Mulligan, Banham & Findley	Janice F. Mulligan	+1 619.238.8700	usa@lexing.network
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Hongrie *Hungary*	OPL - Orbán & Perlaki	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde *India*	Poovayya & Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Luxembourg *Luxembourg*	Emmanuelle Ragot Lawyers & Associates	Emmanuelle Ragot	+ 352 661 84 4250	luxembourg@lexing.network
Maroc *Morocco*	Elkhatib Lawfirm	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Knut Fiane	+47 21 93 10 00	norway@lexing.network
Philippines *Philippines*	Calleja Peralta Jimenez San Luis Uy & Ulibas (Calleja Law Office)	Anthony B. Peralta	+6336113 +6352307	philippines@lexing.network
République tchèque *Czech Republic*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	czechrepublic@lexing.network
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Rwanda *Rwanda*	Siewe William Walter	Siewe William Walter	+(250) 787 642 337	rwanda@lexing.network
Sénégal *Senegal*	SCP Faye & Diallo	Mamadou Seye	(+221) 33 823 60 60	senegal@lexing.network
Slovaquie *Slovakia*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	slovakia@lexing.network
Suède *Sweden*	Eris Law Advokatbyrå	Katarina Bohm Hallkvist	+46 (0) 70 646 6768	sweden@lexing.network
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan. Directeur de la publication : Alain Bensoussan - Responsable de la rédaction : Isabelle Pottier Diffusée uniquement par voie électronique - gratuit- ISSN 1634-0701
Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/